Meeting Minutes
Friday, November 22, 2013
9:00am – 3:30 pm
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

These meeting minutes are a general record of the participants' discussions during the meeting. The notes follow the order of the meeting agenda and use some paraphrasing. The webcast and all meeting documents can be found at www.smartgid.gov/privacy.

Welcome and Opening Remarks
Eric Lightner, Department of Energy Office of Electricity Delivery and Energy Reliability, Director, Federal Smart Grid Task Force

Mr. Eric Lightner welcomed participants to the third multistakeholder meeting for a voluntary code of conduct (VCC) around data privacy. Mr. Lightner explained that there has been a lot of work going on by the work groups drafting their principles with a lot of good work done to date. The draft principles for the VCC will be presented publically for this first time at this meeting. I think you will agree with me we are far down the road.
Mr. Lightner explained that the end of the meeting will focus on next steps for the VCC (getting consensus, where it resides, how to adopt/implement, etc.).

Meeting Overview and Structure
Ron Binz, Public Policy Consulting Meeting Facilitator

Mr. Lightner introduced Mr. Ron Binz, a Principal at Public Policy Consulting, who was tasked with facilitating this meeting. Mr. Binz served as a Senior Advisor at Colorado State University and as a chairman for the Colorado Public Utilities Commission (PUC). As PUC chairman, Mr. Binz led many policy changes that were championed by Colorado's governor and was also an active member of National Association of Regulatory Utility Commissioners (NARUC), serving as Chair of NARUC's Task Force on Climate Policy. Additionally, Mr. Binz served as President of the National Association of State Utility Consumer Advocates while Director of the Colorado's Office of Consumer Counsel.

Mr. Binz thanked participants for joining the meeting and invited participants in the room to introduce themselves. Mr. Binz explained the procedure for asking questions in the room and on the phone.

Mission Statement Work Group and Facilitated Discussion
Presenter: Dan Francis, American Electric Power
Facilitator: Ron Binz, Public Policy Consulting

Mr. Francis presented updates to the proposed mission statement developed by the work group and thanked members of the work group for their contributions. Mr. Francis noted that the mission statement was edited to reflect issues raised during the June VCC meeting. There was discussion around this is being a voluntary standard, but yet the draft mentioned requirements; the new draft attempts to reconcile this. The Work Group directed questions related to the scope and type of data covered by the VCC to the Data Access and

Participation Work Group. The Work Group also incorporated text developed by the Executive Group, which was intended to provide guidance and direction to all VCC work groups, as a preamble to the mission statement. There was also discussion on the previous version being too utility centric and not addressing third-party up applicability; The Work Group addressed that. Lastly, language in the previous version that only related to state laws and regulation and did not address the other potential jurisdictions; that issue was also addressed.

The mission statement is as follows:

Mission Statement

The purpose of the United States Department of Energy Federal Smart Grid Task Force Voluntary Code of Conduct is to describe principles for voluntary adoption that:

1) encourage innovation while appropriately protecting the privacy of Customer Data and providing reliable, affordable electric and energy-related services;
2) provide customers with appropriate access to their own Customer Data; and
3) do not infringe on or supersede any law, regulation, or governance by any applicable federal, state, or local regulatory authority.

The VCC's recommendations are intended to apply as high level principles of conduct for both utilities and third parties.

The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, it is envisioned that the VCC could be most beneficial to either entities that are not subject to regulation by applicable regulatory authorities, or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines.

The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could potentially adopt the principles of the VCC with some limited exception, such as when laws, regulatory guidance, governing documents, and/or prevailing state/local business practices indicate a different approach. In these instances, utilities or third parties should explicitly note the reason for the deviation(s) and prominently indicate such in any depiction that they have adopted the VCC, such as in a privacy policy or other notice of adoption. Nothing in this VCC is intended to change, modify, or supersede state/local laws or regulatory guidance.

Mr. Francis noted that the working group considers this as their final work – if approved by the leadership group, of course, and subject to reconciliation with other major components of the VCC. The mission statement is also posted on the web as well.

Mr. Binz invited participants to provide comments and feedback on the proposed mission statement:

- We support the mission statement. I would like to highlight a difference between what is listed in the mission statement and the key definitions included in the back of the VCC meeting packet. Under applicability/adoption in the definitions, the first paragraph states:
  "The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, we envision that the VCC could be most beneficial to either unregulated entities or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines." This definition does not seem to be consistent with the language in the mission statement. I would suggest the definition language be changed to be consistent with the mission statement. Saying "unregulated entities" can be misleading because cooperatives and municipalities are regulated by their boards and commissions.
  - To be clear, you are suggesting the definitions in back reflect what we wrote in the mission statement?
  - Correct, just that one phrase
  - Let me just use my prerogative.
  - I put the screen up -- it is this sentence here, the fourth line down from the top.
  - It is envisioned the VCC could be most beneficial to either entity not subject to regulation by applicable regulatory authorities or by those who have not imposed relevant...
  - First of all, the words are different, you are correct.
  - Is the meaning any different between the two?
  - Is unregulated the word that you are focusing on in the definitions?
  - You would prefer to have this instead of the word unregulated?
  - Within the key definition under applicability and adoption, that the second sentence of that first paragraph be consistent with the second sentence under the second bullet of the mission statement, the sentence that begins with "however, it is envisioned --"
  - There are two ways to make that consistent. You prefer to stay with the language on the screen and then use the definitions. I am just anticipating there may be other points of view. Just to understand where you are coming from, how about if it was done in the other direction, would that be OK, would you rather not go that way?
  - We would rather not go that way. Saying unregulated utilities or entities is a term of art. You are either thinking about the ones regulated by the state or it is nothing, but that is not the case. Municipalities and cooperatives have boards and commissions. Taking out the unregulated and then describing them as subject to regulation by the applicable regulatory authorities would be the most consistent and accurate.
  - I am not sure if this an issue for anyone, but if you are a third party provider of smart grid services, would you think of yourself as unregulated? I realize cooperatives are in a different boat. However, no one seems to be opposed to what you have proposed.
  - The language of the key definitions came out of the Executive Group. We should refer to them to comment on this.
- I would like to make sure that we are all on the same page. When I read through the first part of the mission statement, which talks about encouraging innovation while promoting the privacy of customer

data, I have approached the word privacy differently over the past few months. There have been a number of regulatory proceedings for those that have come in and talked about privacy being specific to the residential customer, but it does not necessarily apply to other customers of the utility. It is a valid point that privacy is a term that has largely been associated with the individual, not necessarily with businesses. When I look at the mission statement, I am not proposing that the word privacy be taken out. I want to make sure that we have a common understanding of how the VCC will be applied. Is it just to residential customers, or would it also apply to all customer data? I would propose that if it is intended to apply to all customers, you may want to add confidentiality as typically businesses and corporations have looked at their information as having a confidentiality-type protection to it, as opposed to privacy protection. If that is the direction the group wants to go, I think in the spirit of harmonizing things, we would probably look at the definition and say something other than individual customer to reflect customer usage. When I read these definitions in the mission statement, I do not want there to be any ambiguity when we go to implementation mode. I would advocate that the VCC has incredible value for all customer data and I would be certainly happy to debate with folks about whether they think it should be specific to residential data or another class of customer.
    - That is a valuable comment. We did have a brief conversation on that subject in the Mission Statement group. It was our understanding that the VCC would apply to all customers, not just residential. As it pertains to the confidentiality statement, again, we can offer that up for comment. If it helps to clarify that it would be a broad consideration of the customer that it would apply to, I think that would be a welcome change. We may get into some debate about the issue of privacy versus confidentiality and the technical definitions of those two closely related aspects.
    - After we go through all of this effort, I did not want someone to say this is only for residential customers because of the word privacy being used. I think we can clarify the intent of the scope.
    - May I ask, what you think is implied by the two different words privacy and confidentiality?
    - When this debate came up in a variety of circumstances, we are often talking about the risk associated with customer energy usage data. For some, when looking at the risk from an individual standpoint, the concerns raised were related to knowing when someone is at home, when they are on vacation, and recognizing patterns. This seems to be very focused on the individual as opposed to a company. Commercial customers talk about this in the context of energy usage as a component of their secret sauce. If it is known how much energy they use and what they are paying, that may compromise their ability to compete. In that case, the word confidentiality or proprietary applies.
- We will ask Dan to take these two issues back to the work group. If there is no objection, they can go ahead and make the change.
- Who is taking care of the definitions?
    - It was the Executive Group.
- Dan, would you mind explaining the discussion that your group has had on the slides you shared and explain if there were any issues about whether you could opt out of sections of the VCC with appropriate notice?
    - I think the intent of the overall initiative as we understood it in the mission statement was that we would develop a set of principles that an entity, third party, or utility would decide to adopt or not. We understood very early in the process that there may be reasons why a utility or third party would not adopt portions. It was identified for instance in electric choice states. There may be either state requirements, regulatory rules, or business practices developed between third-party electricity providers and utilities regarding the process of whereby entities get certified by the commission to get data for marketing customers or services. We identified that we would like to

have the ability for those entities to still participate in doors and hopefully adopt the VCC, but that they would have to opt out of specific provisions. There was also a discussion on if they are truly adopting the VCC. We tried to allow for an entity to say yes or say they are not adopting a provision, but explicitly indicate why.

Mr. Binz wrapped up the discussion.

Notice and Awareness Work Group Presentation and Facilitated Discussion
Presenter: Amanda Stallings, Ohio Public Utilities Commission
Facilitator: Ron Binz, Public Policy Consulting

Ms. Stalling presented updates from the Notice and Awareness Work Group and thanked members of the work group for their contributions. Ms. Stalling summarized the set of principles defined by the work group that should be included in the notice. The Notice and Awareness draft principles are as follows:

Requirements related to communicating applicable policies, and related choices, to customers.

1) Principle of Data Management
   - I. Collection
     - Companies should notify customers of the types of information that are being collected.
     - Companies should notify customers, at a high-level and easy to understand language, how their data is being collected.
   - II. Use
     - Companies should inform customers why the information is being collected (e.g., billing, rate structures, federal/state programs, customer communications, and for other purposes outside the normal course of business).
     - Companies should provide an overview of what the data will not be used for (if applicable).
     - Companies should explain how individual level data will be used, including when it is used.
     - Companies should explain that data they collect may be used in conjunction with or merged with other data.
   - III. Security
     - Companies should inform customer of high-level methods for securing data throughout the lifecycle of the data and that their data is secured in accordance with any requirements of applicable regulatory authorities.
   - IV. Sharing
     - Companies should generally notify customers of all parties with whom data is being shared with (service providers, contractors, etc.).
     - Companies should inform customers of the company's duty to respond to certain legal and regulatory requests.
     - Companies should inform customers of the purpose of sharing the data.
   - V. Retention & Disposal
     - Customers should be informed that CEUD will be retained and disposed of consistent with applicable local, state, and federal record retention rules and regulations, as well as company policies.
     - Companies should include a statement regarding the conversion of some data from hard copy to soft/electronic copy.

2) Principle of Notification
   - Companies should provide to customers in generally acceptable formats (i.e., paper and/or electronic) as appropriate and as may be required by applicable regulatory authorities.

- Companies should provide to customers, at minimum, notice at the initiation of service and annually thereafter.
- Companies should make customer notices available online and by customer request.
- Companies should provide materials in various formats that are easily understandable by the demographics they serve.
- Customers should be provided with an updated notification when there is a substantial change in procedure or ownership that would have impact on customer data.
- Notice should include, at minimum:
    - An effective date
    - A point of company contact
    - If notifying of a change in policy, a summary of the changes or a means by which prior versions can be obtained
    - Protections against unauthorized access

a. Notice should be reviewed at least annually and to meet current regulatory/legal requirements.

3) Principle of Customer Rights

I. Rights of Awareness

Customer should be given notice that they have the right to ask the company what data is collected, what it is used for, and who has access to it.

Customer should be given notice that their information may be shared to fulfill a Primary Purpose.

Customer should be notified of their right to consent to the sharing of their data for secondary purposes as outlined in the Principles of Choice & Consent.

II. Rights of Access

- The notice should inform the customer of their rights to access, review, and dispute the applicable data.

III. Rights of Dispute Resolution

- Customer should be notified of their ability to dispute errors and potentially correct those errors in their applicable data.
- Customer should be notified of the company's dispute process, including possible recourses for disputing a company's decision.

4) Principle of Data Classification

I. Energy Usage Data

- Notice should identify source of information (i.e., meters, credit reports, etc.)

II. Personally Identifiable Information
- Notice should identify source of information (i.e., online, consumer hotline, mail, consumer credit report, etc.)

III. Shared Data
- Notice should state the conditions under which data may be shared.
- Notice should explain how company may obtain and/or share information from other sources, as well (i.e., credit reporting agency or government entity, contracted agents).
- Customers should be told what sharing they can opt in to accept and how to do it.

IV. Aggregated Data
- Inform customers that Aggregated Data may be used and shared to fulfill certain business purposes.

5) Principles of Customer Awareness

I. Data Collection
- Companies should be able to educate customers about any questions they have regarding the reasons for data collection.

II. Privacy Rights
- Company should inform the customer, broadly, of their privacy rights.
- Company should inform the customer of ways to access privacy policies, rules, and/or notices.

III. Customer Responsibility
- Customer should be educated on what their responsibilities as a customer entails (e.g., providing accurate data, notifying company of changes to data, etc.)

Mr. Binz invited participants to provide comments and feedback on the proposed principles for notice and awareness:

- Under the principle of data management, there is a similar reference under the security section and the retention and disposal section that is slightly different. In both of those areas, there is a reference to consistency with local, state, federal rules, and requirements of applicable authority. That type of language does not inform people of what the method is for security and does not really inform people of what the actual retention policy is. Is this the actual language you are expecting to be in this principle or will it explain how they are retaining and securing it? I have always found that vague language can be very meaningless to the customer.
  - I understand your concerns. Are you talking about retention and disposal, not security?
  - "Applicable authorities" is used under security also. If you are using that language and you do not have any further reference to what those requirements are, you are basically telling people, "we

are securing it in accordance with regulatory authorities, but we are not telling you what those requirements are."
    - It would be the company's responsibility when the customer asks what the applicable authorities are, it would be their responsibility to tell them that they stored data and they have a retention policy in accordance with what authority.
    - This is a principle. This is what the company is agreeing to. There is the secondary step of how it is communicated. That is where I see some potential gap in terms of if the company is required to say something like "we are going to do it with applicable authority." We would expect a company signing on to the VCC to say what they are doing and what is required from the applicable authority.
    - It is the company's responsibility to use these principles and to take it a step further for the customer to be able to interpret and understand the principles.
    - I guess it is a question of whether that will be clear. As businesses sign up on these principles, they have to take that secondary step. That is my comment on that language. I understand the difficulty. I am just wondering if some further step needs to be said to the businesses signing on to the principle.
    - You are on a phone call with a customer and the customer says "what are you doing to protect my data?" What would you like the principles to be required to say, what kinds of things?
    - This is how we are securing it. Not to say we are securing it in accordance with applicable commission requirements or we are securing it consistent with federal policy. I do not want this principle to be read so that a business would say the way I carry this out is my customer service rep tells a person, we are securing the data in accordance with applicable regulations. Does that make sense?
    - I understand exactly what you are saying.
    - Regarding your issue of security, we had a heavy discussion over security, because it is the buzzword of the day. Customers are starting to become more aware of it. Customers need to know that their data is being secured, but it was a decision of the group that customers do not need to know exactly how their data is being secured. For example, a customer does not need to know that their data is being secured using encryption software. It leaves them and other customers open to vulnerability if another customer finds out what they are using to protect their data and they happen to be a hacker. That is why we say at a high level, customers should be aware that their data is being secured, but that does not mean that you give the customer the how-to book on how your data is being filed.
    - I understand that with regard to security issues.
    - Companies should inform customers of high level methods for securing data throughout the lifecycle of data. That has got to be an answer different from whatever the PUC told us to do, isn't it?
    - It should be. Point taken. I would like to keep that on retention and disposal. It would be consistent with security and then it would be consistent with the applicable authorities. You are right, security does have the two steps.
    - The work group will go back and review this issue.
- I want to make a follow-up comment to the previous point that might be helpful. I understood the concern was in the security and the retention and disposal principles, the second phase of that, we will inform the customer that data is secured in accordance with the law. It will be disposed of in accordance with the law. I understood your concern, and please correct me if I do not understand it correctly. Is that what language goes into the notice? If the language says we are going to retain your information in

accordance with the law, what does that tell the customers? We have some intention because we often have companies' policies that are criticized for being too long and too detailed and it is not clear and concise. So appreciating the point of a customer that might want to know what those requirements are. A utility or another company generally would provide a customer who requested it. One alternative could be we want to consider such requirements could be made available upon request. I do not think we need to inform all the litany of document retention requirements in the policy itself.

- I have a question under sharing. The first principle says that companies should notify customers of all parties with whom data is being shared. There is a parenthetical. I will state my concern and then I will highlight a couple of other instances within these principles where it comes up. When you are talking about small utilities, the idea of notifying customers with a great deal of specificity is a concern. My question about this language is, how does the group envision that it would play out in terms of what constitutes generally notifying customers of all of the parties?
    - I do see your point. We need some clarification in the principle. I believe when we were discussing this, customers do have the right to know their data is being shared with other parties. Maybe not specific like, "we share your data with Opower." You can tell a customer we share your data with contractors who we contract with to provide services. We share your data with third-party service providers who we have business dealings with. Maybe not down to the company name, who this person is. A customer has the right to know if their data is being taken outside of the company doors to fulfill a business purpose. Maybe not the name and location of the company to that specificity. The customer should know their data is being shared with contractors, other service providers the company may have dealings with. I think we need to go back and try to get that across because it maybe unclear.
    - Reading this principle with others and the description of what constitutes notice that made me scratch my head about whether or not we were journaling down too much in terms of specific information. They frankly do not have the resources to provide it and customers maybe not care.
    - Your average customer says where is the dollar amount and who do I write the check to? If the customer wants to know they have that right to be informed and the company should inform them. That is where we were coming at it.
    - We are talking about two different levels of engagement. Earlier we said this is in the context of a subscriber signing up for service and affirming the customer understands the implications. Let's agree, a lot of customers would never even think about some of these things unless they are told about them. That is really the point. Utilities are mysterious beings to many consumers and to know that Excel Energy or FirstEnergy contracts with OPower, it may not occur to customers that this even happens. I take your point but we need to understand the purpose of this clause is to make sure that disclosure and notice is sufficiently filled out. I agree with the thrust of your comment that we do not want to try to make it detail everything. You need to be clear. That will be real important if you expect to defend a customer's permission as being fully informed.
    - There was an issue in Ohio where a company had contracted with a third party service to compare energy usage of neighbors as a part of their smart grid pilot program. We did have issues with customers contacting the hotline that they received a smiley face or a sad face saying "you are using more or less than your neighbor." The concern was, who is this company and how do they get my information? Again, we all pretty much agree on, your average customer, the utility company doesn't mean much to them. The company needs to be informing their customers about that. An educated customer is a happy customer.
    - That's fine. I think we can find a common ground.

- Is there any thought about passing on the requirements of the VCC to contractors? When you use health data, there was an agreement that requires you to follow everything that the person who works with what they had to agree to. It is like a trickle-down control of security. Has there been a discussion of that?
    - I cannot speak on behalf of the entire VCC. From what I understand with utilities and working at the Ohio commission, it is pretty much normal and regular for a company to require the contractors to follow their business principles in order to do business with that contractor. If a company agrees to follow the VCC, they will want their contractors to follow that as well.
    - Would that create an obligation? If and when we do share with contractors they are subject to the same obligations that we make to you by signing this in the first place?
    - We didn't think that it was our place to tell a company what they can do with their contractors. It should probably be covered by the VCC executive management team. Or maybe even it should be something the company discusses with their contractors as part of doing business. I do not think we can make that decision based on the entire voluntary code of conduct.
- In the third principle of customer rights, the last bullet point says the customer should be notified of the right to consent to the sharing of the data for secondary purposes. I was a little confused. Companies have to seek the informed consent of their customer before this data can be shared for secondary services. That is something you can exercise if you want to. The underlying thought is we are going to seek this consent before we do this. It is more of a requirement for companies to seek the consent and then the customer to give it. Does that make sense?
    - The customer has the right even after the initiation of service. We were looking at it from the entire business relationship cradle-to-grave and then it is done. Should a company be asking a customer before they start sharing data? Yes, they should. A customer should still be notified of their right to consent because they do have that right to consent.
    - Maybe it is the word "consent." Consent is an action. I guess that is how I understand the term to mean. I think that the right to consent is the most clear way and you don't know where the obligation lies. "I have a right to consent" and the company goes, what do you mean, consent?
    - Right. Maybe it can be modified or add a sub bullet that states the customer should be asked to consent prior to the sharing of data.
    - A right to control on the customer side or a requirement to seek the consent on the company side.
- Regarding the second page under the principle of data classification, the last bullet point under shared data says ‘customers should be told what sharing they can opt in to accept and how to do it.’ This says to me that what we wouldn't share with the customers is an opt out? I'm guessing how you guys envision it is the utility would say these are the things you can and cannot control because there are some things we have to share regardless. Is that what you are looking for there?
    - A customer should be able to know what services they can opt in or opt out of and what services they cannot opt out of. If there is a third-party service contractor for billing purposes and the customer says I do not want my data shared, yes. The customer should be told if a concern is presented. The customer may not go into detail but they may. They should understand and be informed that there are some services you cannot opt out of.
- I am looking at the notice and awareness section under the principle of data management and retention and disposal. It says this should be a statement regarding the conversion of some data from hardcopy to soft electronic copy. I am wondering what the rationale for this is. Many companies are moving rapidly toward almost automatically having the data electronic. If you have a call center and a person calls, there is no paper involved. They are entering that data into a database right then and there. I do not understand the rationale behind it. What is the need for the notice if we envision a world in which

everything will probably be electronic and not just in the utility industry but everywhere? The other issue is what is some data? Which data are you talking about that would be captured if there is a rationale for this kind of notice?

- When we were talking about this, we wanted to include all of the possibilities that we could think of. One of the possibilities is if you have a small utility company, only referred to as mom and pop service. They may ask them to use a paper application and scan it into the system or electronically enter the data when they receive the application from the company. There are still companies that are like that. Going back to what we know and what we don't know, you do not know information the company is going to want to convert. It is different for every company. We didn't want to specify what data but perhaps a way to make this better and to clarify what, instead of saying some data. The company should inform the customer of what those electronic conversions would entail, basically saying what data would be converted.
- I still do not understand why. Why is there a need for the customer to know whether you keep a paper record or electronic record? Especially when we know people are moving toward electronic. If you have a website and a person can sign up for a service on the website, I think that person should know that they are signing up electronically. Do you want the person, the company to say you are signing up electronically? That is why I am asking why. Is that conversion something important?
- There are certain customers who do not embrace electronic conversion, who still want to have a paper copy. They write a check and slap a stamp on their bill instead of doing electronic banking. I think that you have to include this case. There are still customers out there who do not understand that if they submit something in hard copy it is going to be converted to electronic copy. Some customers do not want their hard copy converted to electronic copy. Going back to the financial sector, I believe because we have this happen in our personal level, there are customers who didn't want their checks converted electronically. They want their canceled checks back to them at the end of the month rather than receiving electronic visions or electronic copies of those checks. We need to cover that in there. There are a variety of opinions regarding electronic conversion data security. I hope I was able to answer your question.
- What you're capturing seems to be moving further than privacy because those types of transfers always existed. It is moving into whether a customer just doesn't like electronic handling of data. I understand what you are saying, I just do not agree with the purpose.
- If it is a utility or vendor document, it is hard to understand why the customer has a stake in how that is stored. It cannot surprise people anymore that a document might be scanned and maintained electronically. The question is whether it is a consumer protection to tell them that fact in advance so that they can opt not to take the service because a contract they signed is going to be stored in a database? The work group will take this point into consideration.

- I think I agree with where the work group said I believe it is appropriate for the service provider to give notice to the customer that they may be sharing their data with contracted agents. I do not mean this to be a spoiler, but my work group looked at that in the context of primary and secondary purposes and in the context we proposed we talked about specifically contracted agents of the service provider that support a primary purpose. I think from a notice standpoint we need to give notice of that. I would discourage listing all potential contracted agents. I think that would be burdensome from a small co-op standpoint but also from a big company standpoint. There could be many and keeping that list current would be problematic. Under the spirit of transparency, we should disclose that. Some of the discussions may have muddied the waters a little bit. A lot of what the VCC talks about is giving the data to third parties. I want to make sure we keep some delineation between third parties and contracted

agents. We cannot give customers the opportunity of opting out of data sharing with our contracted agents that prints and mails are bills. Opt out is not going to work there. You have a contracted agent versus a third-party. I think the thing that folks might have been looking for is if the service provider sharing that information with the contract agent. Are we putting that data at risk? The customer does not have the option of opting out, opting in. Is there a risk? I would say that lands more in the data access group than notice. That is not addressed in our principles that we have; we can take that back to our workgroups when that information is shared and not subject to the opt in and opt out. I think most states that have looked at this have found that there should be. So I make that offer. We can talk about that further. It seems like it is more of a data access issue. On record retention requirements, that falls into our group. Our schedule listing for state and federal retention is 550 pages long. From a transparency standpoint, it is important to talk about how retention is going to be governed. Sort of the same thing with your contracted agent. I am not sure the value will be listing the specifics.

- I am concerned about the principles of notification. The company should notify customers at a high-level and in easy to understand language how their data is being collected. I do not know what high level and easy to understand is in the world of smart grid on how their data is being collected. I think that could be onerous at best if I try to explain to customers that the data travels from meter to meter until it gets to a collection point and it goes across to a cell tower and into a data collection engine. Do you want me to tell customers that? This is about smart grid and these are the things that customers are concerned with. Are you collecting it through a radio frequency or cell phone? How are you collecting my data? Is that the concept you are trying to get across here? This is around smart grid and customer energy usage primarily. The privacy policy explains how the data is collected. I think that when you get into notification, you talk about this annual notification and open enrollment and I think that is onerous at best. I would think I should be able to put my privacy policy on my website and consumers that want to view it can. As a utility in Texas, I do not know the mailing address of consumers. I cannot mail them anything. You talk about companies at the initiation of service. I do not know what initiation of service means to a third-party it might be the service they are offering. To a utility, what is a service? I think we need to be cautious with that for your competitive markets because if I am a consumer in Texas and I sign up with an energy service provider and they sent me a notice and then the utility sends me a notice of their privacy policy every time I switch providers, and I can switch providers every day.
    - I disagree with you. I think every time a customer switches companies, the utility should provide it.
    - We do not have a business relationship with the customer at the utility. We are more like a third-party. I just do not think it is clear what the utility would be.
    - I am concerned, and maybe this would be one of those things I would opt out of as a utility. I'm going to abide by these principles. Customers should make it available online and by customer request. What if the company does not have an online method? I think that is problematic. I think it is onerous in the way it is stated.
    - You are not required to give them a notice every time they change service providers. The relationship between the customer and the third party servicer changed. The business relationship did not change between you and the customer.
    - If you would merge with another company and there were substantial changes in the company structure, yes, a notice would need to be mailed to the customer. There are many customers who do not have access to the Internet.
    - I do not know their mailing address in Texas. I know some of them if they get their mail at their service address. I just think it is onerous.

- On the sharing discussion, I thought it would be helpful to say on that first point that the company should notify customers of all parties with whom data is shared. I agree with a lot of the comments that a substitute informs the customer and we share information with our service contractors. Information is available on request. Not specifying who they are seems like a reasonable thing to do. With regard to the comments just now, I am concerned because I understood the utility would have a distribution service relationship with the customer. Companies do this all the time now. You sign up as a customer and you get a notice and they give them a book or something saying we keep your records for x, and that is all they do. And the supplier relationship is something else.
- I agree with your comments. Each third-party under this would have responsibilities to notify the customer. That was my understanding of what you are trying to do here.
- Under section number 2, the list of things that a notice should include at a minimum. What effective data are you talking about? Can we make it as generic as possible, consistent with the conversation?
- I have a comment on section four. You are talking about classification. You have a note in regard to personally identifiable information. I have got no problem with notification around the different data that is being collected by the service provider. That is a term not defined in the VCC. We defined CEUD. My group also created a principal around other data, some of which has been defined as PII. I want to make sure we are using our nomenclature in terms consistently here. What we did in my group is we created a principal that basically says the VCC is not talking about this type of data. That is already regulated in other areas. This data is not within the scope. The sharing of this data is not governed by the VCC. I have no problem saying you need to give notice of your data practices. Do we say you also have to give notice of your data practices around data that the VCC is addressing and we have a proposed principle that says we are not addressing this? Just a point to consider for the workgroup.
- I was wondering if you looked at all when it is providing the groups of data in Illinois right now, groups of customers to third parties. We are not talking about aggregated data or account number and address. And if there is any protocol surrounding that.
    - I think your question is going to be better addressed when we take up that discussion. I have been up here a couple of times. I do think you will not be dealing with one who wants to talk on this topic. We should take it up when we get to that part of the day's agenda.
- I do not think at any point in our discussion we talked about identifying each company. And perhaps one of the faults is that we are probably too generic and people think we are too detailed. People do seem to want more detail. At no point were we thinking about a detailed list of third parties. I would agree that that is a little ridiculous. Customers should be aware of the nature of buckets of services that you may be sharing information with. In response to what the notice should include, I am struck at the idea that the things we're doing around notices is not at all new. We all receive notices from our insurance companies, our telephone companies, our cell phone companies with notice statements. None of this in the notice section is new at all. This is long-standing notice provisions in other industries. We are now just catching up to what has been done in other industries.

Mr. Binz concluded the discussion on the notice and awareness draft principles.

Management and Redress Work Group Presentation and Discussion

Presenter: Chuck Piotrowski, Green Mountain Power
Facilitator: Ron Binz, Public Policy Consulting

Mr. Piotrowski presented updates from the Management and Redress Work Group and thanked members of the work group for their contributions. He explained that the work group reviewed the set of comments made

during the last meeting and determined that they did not change the tone or nature of the draft principles. Therefore, no changes have been made to the version presented at the previous meeting [June 4th]. The principles for management and redress are as follows:

1) Company Management and Customer Redress
   - I. The organization will regularly review its information practices for process improvement opportunities and compliance.
   - II. The organization will take action to meet legal mandates and ensure when necessary appropriate privacy practices.
   - III. The organization will provide a simple, efficient, and effective means for addressing individual customer concerns. This process will be easily accessible to the customers and provide timely review, investigation, documentation, and, resolution of the customer's concern.
   - IV. On all issues above, the organization will follow existing procedures established or approved by the Applicable Regulatory Authority or Governing Documents, if any. Meeting such applicable procedures will be sufficient to demonstrate compliance with, or under, the VCC.

The management and redress principles were meant to guide organizations, while being flexible enough to allow companies participate in the VCC and to self-monitor themselves. The wording included in the document is very deliberate to reflect that an organization will follow the VCC principles and regularly review their compliance. The work group did not want to prescribe what level of frequency these reviews should occur. The principles also reflect that organizations will take action to comply with legal mandates, when and where necessary.

There were no questions or comments on the proposed set of principles.

Choice and Consent Work Group Presentation and Facilitated Discussion
Presenter: Susan Neel, CenterPoint Energy
Facilitator: Ron Binz, Public Policy Consulting

Ms. Neel presented updates from the Choice and Consent Work Group – on behalf of Eric Ackerman the Work Group lead – and thanked members of the work group for their contributions. The primary focus of this area was around how a customer can choose and consent to their energy usage data being distributed to others. Ms. Neel presented the proposed principles along with several examples to help explain their meaning. The proposed principles are as follows:

Policy principles related to the customer's granting of authorization for the release/sharing of his or her data.

1) Principle of Customer Control
   - Electricity distribution companies require access to customer energy usage data as a condition of service.
   - Customers should have access to their own energy usage data.
   - Customers should have the ability to share, or not to share, their energy usage data with third parties.
   - Customers should have the ability to authorize differential disclosures of their energy usage data among multiple third parties.
   - Customers should have the ability to rescind disclosure authority previously granted to a specific third party in a manner that is convenient and easily understood.

2) Principle of Informed Consent
   - The processes by which customers exercise informed consent should be convenient, accessible, and easily understood.
   - Customers should base consent decisions on an understanding of specifically which of their energy use data is proposed to be shared with a given party, for what purpose, and for how long.
   - Customers should base consent decisions on an understanding of all disclosure-related choices available to them.
   - Customer consent should be specifically and affirmatively expressed.

3) Principle of Valid Consent
   - The processes by which customers exercise informed consent should be secure so that customers are protected against disclosures based on fraudulent consent.
   - To the extent a process is needed to ensure the validity of customer authorizations (on-line processes may be secure without additional validation), privacy policies should clearly define the party responsible for conducting such validations.

4) Principle of Controlled Disclosure
   - Disclosure should be limited to that energy usage data which the customer has authorized for a specific party for a specific purpose. Authorized parties can disclose CEUD to their Agents.
   - Any party that discloses CEUD should retain, or cause to be retained, a record of disclosures so that customers can identify all the parties receiving their energy usage information, and ascertain that disclosures were given consistent with regulatory requirements or industry standards, as appropriate.

- A duly authorized disclosure should cease when (a) the customer rescinds his or her authorization, (b) the authorization expires, or (c) the customer terminates electric service.
- When an entity receiving duly authorized CEUD is sold, the party providing the CEUD is not required to notify the customer of the change in ownership, and the new owner can continue receiving CEUD without the need for a new disclosure authorization. However, the entity receiving CEUD must notify the customer of the change in ownership.

5) Principle of Efficient Management
   - The business processes supporting consumer choice and consent should be cost efficient, and utilize standard formats.

Ms. Neel also presented examples developed by the Work Group.

Mr. Binz invited participants to provide comments and feedback on the proposed principles:

- I want to bring up a concern on the third bullet on customer control. The customer should have the ability to share or not share energy usage data with third parties, and I guess our concern would be working with contracted agents, billing agents, that the customer should have the ability to not share energy usage data with contracted entities for those purposes?
  - We've had this conversation over and over again. We are hoping in the definition the contracted agent is not a third-party.
  - Way back, I think we agreed in general to that concept. So, the agent is an extension of the utility and all rights and responsibilities pass through that relationship. So, this was actually raised earlier today. You do not get out of your obligations under VCC merely by shifting the data to a contracted agent. Those obligations still apply to the utility and vice versa.
- I have an amendment to propose. I'm thinking given the scope of what you have looked at, under principle four, the principle of controlled disclosure, you talk about a situation where the third party has a change in ownership. So there is a data flow going from the service provider to the third-party party and the third-party has a change in ownership. You are saying the responsibility for the notice is with the third-party to the customer, to let them know they were bought by a different company. The only thing that I thought of when going through that is, it may be helpful to require that third party to also tell the customer how they could revoke consent if the change in ownership is at all meaningful to them. You talk about the fact that there needs to be the opportunity for the customer to revoke. In this particular situation, learning there is a change in ownership, it may change how the customer feels, and I think notice should also be meaningful enough to tell them what they can do about that if that makes a difference to them.
  - Makes sense to me.
- On the same bullet, the way it reads right now, the entity must notify the customer of the change in ownership. To the extent that the entity receiving this is again a contracted agent, I am presuming this sentence will also be squared up with all the other sentencing we have got in here about who has to be informed. When do you or do you not need consent? If you have a contracted agent for billing services and that contract goes to somebody else, we don't think that the new billing entity should be in touch

with the customer and certainly the customer should be given the opportunity to revoke any sort of rights for that billing entity.
    - So, do you think if we change the duly authorized part to third-party that would take care of that?
    - If we will be squaring up the definitions of third-party and all of that, I think it will fall in line. This is a little bit of a different twist on that because it was not sharing per se.
- I have a question on the bullet we were talking about. As a person who works for a regulatory entity, I feel I would be remiss if I did not point out the regulator or other legal determination. I would suggest that we add some legal or regulatory term on determination of access.
    - I think you are right. If we had a third-party that was a bad actor, I think we would have some legal action to say we would release data. I think that is appropriate. I do not know what my team thinks.
    - So let me make sure I understand this. This is any duly authorized disclosure? So any duly authorized disclosure should cease when one of these things happen.
    - Correct. We have gone through this exercise at least in California. There is an opportunity, we are finding by regulatory entity or court that finds in fact the third party is in violation of some rule or law. The access to customer data should then be shut off.
- My comment or question is around the fourth bullet point. I understand the intent of the original disclosure and flexibility. There does not seem to be a counterbalance around the reasonableness of the request. For instance, you may have a situation where a customer says there are three parties I want. I want this party to get usage and voltage data, and I want this party to get only odd month's energy usage. Unless I am missing it or perhaps it is stressed someplace else, there is no recognition of the fact that there can be a reasonable determination of what should constitute a sort of standard data request.
    - It did. We hoped we had that addressed in the principles of efficient management by utilizing standard formats. Maybe that is not clear. I do not know if you think the principle of efficient management makes that clear, or if you think we need to slip some kind of language that the different disclosures would be.
    - I think a line about options would be helpful.
    - OK.
- The second issue I had was whether or not you got into the idea of customer data versus data that is created as a result of that customer's interaction with the business.
    - We did not get into that. I understand what you're talking about. In fact, I have dealt with the situation where customer had to investigate the data from the sensor on the line that they thought someone had hacked into and was causing the circuit to operate which was causing their security system to go off-line and the ex could not get into the house. Is that what you are trying to explain, that type of data?
    - Yes, there is a whole host of data types, quite frankly. So, what is the voltage fluctuation on the transformer? What might be causing that voltage fluctuation?
    - Versus the meter?
    - Exactly. What if you create a multi-profile for a multi-use building? The data that drives that is the customer data.
    - We did not get into it in Choice and Consent. I think it is a definition issue on what is customer data versus utility data. Even though there are times, like in the example I gave you, where the customer felt their privacy was being invaded because of the result of data we had on the utility side. I can tell you in that process, we did not reveal to the customer the sensors' algorithms or anything. But we did document for them that we had inspected the sensors in a statement. So, I don't know where that really should be addressed.

  - Yes, there's also the issue of the customer having a voltage fluctuation on a circuit and another customer having an impact on their voltage delivery. I don't know that we want to get into that level of detail, but those are issues I at least identified in the broader perspective of what is customer data versus the data product of a provider of any sort.
  - I agree with you. I do not think it is a choice and consent issue, but I do think this is an issue that needs to be addressed around VCC, since it is around smart grid. It is not around the utility of 10 years ago. That is, from what I am seeing, the complaints we are getting are those types of complaints. It is not around my monthly usage data. It is around the sensor equipment causing my security system to do this, or when the RF was sending the signal across the mesh, the customer down the street got the usage data. Those are the kinds of complaints we are seeing.
- I thought I would express support for the suggestion on the phone. I think we all would act in compliance with the law and regulatory authorities, but adding the sub D in there makes it clear. I did have a suggestion. The last bullet under controlled disclosure with the entity receiving dual authorized data. I think we all understand we need to define that contractors are considered part of the service provider. We can't just put a third-party there instead of entity, because the service provider adoption of VCC might be a third-party and not a utility. I think maybe one way you can do this is to say when the service provider is receiving duly authorized information; make it clear that the contracted agent is not the service provider. This leads to a more global comment that I think it might be a good idea at some point to go throughout this document, and I would suggest service provider as a term as a good way to determine the entity, utility or third-party, adopting the VCC. If we make that vocabulary consistent throughout, it might clear up a lot of confusion.
- My concern lies with the language in these principles that you talk about the disclosure to specific entities for specific purpose. I have concern about how that specificity may mesh with other jurisdictions that make customer usage data available to a class of service provider. I will take Pennsylvania as an example. In Pennsylvania, third-party retail electricity and gas suppliers are able to obtain customer list on a regular basis that do include 12 or six months of usage data. I would propose to you that there should be flexibility in terms of the specificity with which a customer consents to the release of their data to accommodate a class of providers such as a third-party energy provider.
  - That is a new one, I think. Isn't it?
  - The same thing holds true in Texas. We do not give out lists, like you are talking about. If a customer signs up with a new service provider, that service provider can get their usage data and their historical usage data as part of that. But we are assuming that agreement in their terms of service with that service provider. What you are talking about is you are releasing this for marketing purposes, right?
  - That is correct. So, I think the principles should accommodate policy decisions that are made in certain jurisdictions. The disclosure of usage data can be made for customers at the outset and can achieve policy goals in the interest of the state or the jurisdiction to achieve. So again using Pennsylvania as an example that has made a policy determination to let customer data be made available to third parties even prior to the beginning of the customer relationship with them.
  - Then it is about customer consent?
  - There is customer consent in that. The customer is able to consent to their usage information being shared with the class of service providers. I think there is a discrepancy between that principle and the principle outlined here it talks about the customer being able to disclose information to a specific provider. I think that there is a specific provider. I think that there ought to be room for that disclosure to a certain class of provider.

  - These principles are not intended to conflict with applicable regulatory decisions and so forth. It seems to me this would not stop this, but you are asking a good question. We should think about this. Whether we want to signal anywhere that we understand that might happen. The Pennsylvania example is a good one. I do not think we have heard this. Looking around the room, I'm not sure we have talked about this before. There might be a place in here.
- In response to that, I was going to point out that the concern is partially taken care of in the mission statement paragraph. Frankly, I would be concerned about adding more and more language to these rules about obtaining consent from consumers. The rules can get changed or you do not require the consent on data. I understand for me this is a strong policy issue on getting affirmative consent. I think to accommodate regulatory or statutory differences within the states is in the mission statement. The mission statement says the utility has to give away the information. That is the reality and it is acknowledged in the mission statement. But I do not think the purpose of the voluntary code of conduct in and of itself, setting aside statutory regulatory authority, is to support the customer's control over access to the data. I would rather not see as a battle from that. I think it is covered in that mission statement.
- In California we have a similar rule to Pennsylvania where an electricity service provider is allowed to obtain customer usage information. But where I think we are OK, not only in the beginning of the mission statement, but also in discussion of primary purpose, we have added a section allowing for meeting a state or federal law or rule. I think that there is already plenty of coverage in the mission statement and the definition of primary purpose.
- There is a little bit of piling on. I just want to say, we fully recognize that there are states that have state policy decisions about who has access to data. If we try to stop the language and the principles we have here, then does that apply to a group of Internet service providers? It starts to then look like it could be applied more broadly. I know in different proceedings I've been in, people come in and say, “could the customer just send a giant, general I agree to share my data with whomever?” To me that raises whether it is truly transparent to the customer who is getting the data, what they are using it for, what their remedies are, that sort of thing, which you have accomplished if you have informed consent. I think we should acknowledge that Pennsylvania and other states that have something like this with a policy decision made, but I believe that all of the decision is appropriately limited to achieve a certain market access objective for the state or could be narrowly provided for specific bodies.

Mr. Binz concluded the discussion of the choice and consent principles.

Integrity and Security Work Group Presentation and Facilitated Discussion

Presenter: Brandon Robinson, Balch & Bingham LLP, representing Southern Company
Facilitator: Ron Binz, Public Policy Consulting

Mr. Robinson presented updates from the Integrity and Security Work Group and thanked members of the work group for their contributions. The goal in drafting these principles was to leverage existing resources and look for nonspecific, general guidance to maintain flexible and adaptable principles versus prescriptive ones that could be a hindrance. The draft principles are:

1) Security and Safeguards
   - I. Data Security Methods
     - Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, related entities and customers.
   - II. Data Protection against Loss, Unauthorized Use, Modification, etc.
     - Implement and maintain process, technology, and training measures to ensure data integrity and protect against loss and unauthorized use, access or dissemination.
   - III. Define Process for Handling Data Breaches
     - Maintain a comprehensive breach response program for the identification, containment, mitigation, and resolution of any incident that causes or results in the breach of data security.
   - IV. Define Process for Customer Notification of Data Breaches
     - Customers should be notified when it is reasonably likely that their personal information has been accessed without authorization under circumstances which may result in misuse of CEUD or Account Data.
   - V. Define Responsibilities for Data Breach Notification and Remedies
     - The Service Provider whose customer's information may have been compromised has the primary responsibility for ensuring the delivery of complete, accurate, and timely notice to the customer and remedying the conditions which led to the breach.

2) Data Quality and Accuracy
   - I. Data Quality
     - Account Data and CEUD should be reasonably accurate and complete, considering the circumstances and environment in which it has been collected (e.g., validated data, data collected indirectly from another entity, etc.). When a Service Provider has modified or enhanced data that it initially received from another source (e.g., a utility or a different third party), the customer receiving the enhanced or modified data should generally be made aware that such data may differ from the initial data.
   - II. Data Accuracy
     - Utilities and third parties should provide a process for customers to dispute the accuracy or completeness of their own Account Data or CEUD, and to request appropriate corrections or amendments. Existing procedures for addressing other types of customer complaints may be adequate.

Mr. Binz invited participants to provide comments and feedback on the proposed principles:

- On integrity and security, it lacks the need that data should be provided. I would like to see more detail on when notice should be given to customers. Different states have laws on how data breaches have occurred. It is not clear that reasonable is an appropriate measure for something as serious as security breach. I'm glad there is reference to cyber framework. DOE has done good job on NISTR7628 and risk management process
    - I understand you want to see language about regular privacy audit or review. We will try to address this. We didn't include it in integrity and security working group. Some other groups might be addressing regulatory privacy audit or review.
    - As for data breach notification, different states do have laws. To the extent that there are definitions by state law, who would answer the question of what is reasonable under the VCC. None of this would conflict with any state notifications.
    - The DOE documents are good to look at. There are certainly aspects we could consider including
- Regarding the issue of when breach notification has to occur, the principle is broad and in terms of account data and CEUD. Do we intend to harmonize this with applicable laws and state laws that wouldn't require notification under every instance of CEUD? My overall comment is whether the intent is to harmonize standards with applicable state breach notification requirements. The notion is usually something likely to harm an individual.
    - Would usage data fall under those state rules?
    - Not always. The California law comes to mind. Something like zip code or email address but nothing more wouldn't trigger that requirement. I'm not sure where we draw the line
    - Changes in ownership, changes in policy or procedures that affect privacy that come into play here. Many data breach notification laws are tighter than what we have here. We intend to defer to policy of the state to decide what is reasonable
    - We need to clarify how this applies to businesses. That's another example that deviates from states. I think that there is cause enough to take a closer look at it.
    - Energy usage data for businesses could be very hurtful. Some might argue that it is more damaging to businesses that to homeowners
- I've look at data breach readiness in 48 state laws and these are not consistent. They address different elements. Some outlier states include different elements. My recommendation is the PII is not clear in this context and CEUD. It is easiest to not try to harmonize state laws on how they define things. Step into where there is a void and make this specific to the CEUD. This is all over the board at different state levels, there will be pitfalls and conflicts. Focus on what the requirements are around data security breach of CEUD and add something on upon discovery. Once it is discovered, they should act quickly and provide notice. I recommend taking out the personal data reference and keep it narrowed on CEUD.

Overview of EERE funded Aggregated Data Project at PNNL

Presenter: Cody Taylor, U.S. Department of Energy Office of Energy Efficiency and Renewable Energy

- Good afternoon, everybody. I hope everyone enjoyed lunch. It's a pleasure to be here.
- I'm with the Department of Energy building technology's office and I wanted to give a quick update on a bit of research work we are sponsoring right now that I think is germane to some of the conversation here today, especially some of the upcoming conversation this afternoon. This study is a bit of work we are doing at Pacific Northwest National Lab over a number of months.

- Our objective is to determine whether data from a large number of real buildings can actually inform policy decisions about data access and customer privacy, and whether that has anything to tell us. If it does, we will try to analyze the difficulty of identification at various thresholds of tenant data aggregation.
- We are really focusing on commercial buildings, the use case of whole building energy benchmarking, because that is something that a lot of commercial building owners are taking more and more interest in today as an energy management practice, and in order to accomplish that, the owners need access to energy data for their whole building.
- In cases where tenants have their own individual meters, that can be a challenge for the owner to get a grasp on what the energy use of their whole building is. The owners are seeking monthly poll building data.
- That is our scope, which I recognize is pretty restricted in comparison to some of the things you all are talking about here. We're not trying to cover the waterfront on all possible use cases, we are just thinking about that particular one.
- Our emphasis is on thinking of minimum thresholds for tenant data aggregation, such that building monthly total energy consumption could be disclosed without compromising tenant privacy, but also potentially without requiring individual signatures from tenants.
- The reason for exploring this is because that is an approach that has been taken in a number of states to date.
- We are trying to see if our research work can help inform future conversations about that.
- We have pulled together a couple of data sets, many buildings with multiple meters from a couple of utilities that we were able to have access to at the national Lab with all the identifying information removed, to understand the patterns of energy usage among multiple metered, multitenant buildings.
- With those two data sets, we have one that includes 1900 accounts with multiple meters, one that includes 17,000 buildings worth of natural gas data, and one with just shy of 10,000 buildings worth of electricity data, just to give you a sense of the scale we are looking at.
- Our analyses are currently exploratory mathematical analysis, looking at variability among the profiles of different buildings, the relationship between building attributes and the attributes of the meters within those buildings, and looking at clustering of buildings into common shapes, if you will, of the energy usage and the way the whole building's shape may or may not tell you something about the individual meters within it.
- We are trying to answer a few questions.
    - What does the whole building's information tell you about individual tenants?
    - What does the building's total tell us about the tenants within it, does it tell us anything about the number of tenants, anything about their usage makeup?
    - Does a building's monthly energy usage data at the whole building level tell us anything about energy usage beyond what you could ascertain from existing public national statistics?
- If all you can learn from whole building data is that tenants in this building used between 10 and 50, and I could have looked up that information in national statistics, that typical building office usage is between 10 and 50, perhaps that does not provide any new information about that building. Those are the kinds of questions we are looking at.
- I wish I was here presenting results, but we are not to that stage yet. The analysis is still ongoing. We only have the first initial look.
- I expect the DOE to have our first draft back from the National Lab next month, in December, at which point we will be looking for peer review and feedback, hoping to publish the final product early next year for everyone's use.

- I'm not sure if the results of this research will provide -- will have a meaningful bearing on the kinds of questions that you are trying to answer here in terms of specific decisions about thresholds for tenant aggregation. We hope it does, but we don't know that it will.
- We are doing this for some of the same reasons that a lot of folks in this room are interested in voluntary code of conduct.
- We understand that customer privacy is important, and something we should protect.
- At the same time, we understand there is an evolution in this space and people's needs and desires are changing.
- This group is doing a lot of work to wrestle with the answers to what appropriate mechanisms are to protect privacy on a large scale, and we hope we can feed into that.
- Our building technology group certainly supports the efforts going on here, and we hope you all continue to push this forward and get to a place where there is a national approach that folks can feel good about.
- With that, I'm happy to take questions.
- I'm sorry I could not bring you more substance to question me on today.
    - You and I had had a conversation, and you said one of the things that comes out of this may not necessarily be a specific aggregation formula or threshold, but that you guys were looking to understand what are some of the risks out there when you are trying to aggregate whole buildings, and may be some things that can be done to mitigate risk. I know that was several months back, and I ask if that is still part of your scope. Do you think that what will be published will maybe say when you are looking at aggregation, here are things you need to factor into that formula or process?
        - The answer is yes. It is part of our scope in terms of the questions we are asking. I'm not sure if we will have anything really useful to say about it. As the statisticians are digging through the data, some of what they could find could say things like, in X circumstances, this is a red flag circumstance where you would want to make sure you're not disclosing data. Something like that might be what we hope to find, but it's possible there's none of that hiding in there and we can't give you anything, but I certainly hope we can.
    - I hope you can as well, because I think that maybe where this group would really interface with the results of your study is being able to say, when you aggregate data, here are some risks that need to be managed. Being able to put out even that level of direction would be incredibly helpful in not only the whole building space, and in the whole data aggregation discussion.
        - I hear you loud and clear.
- Thank you for coming today. I've been looking forward to your update.
- Absolutely. I expect that our final report will come out early in 2014, sometime in January.

Access and Participation Work Group Presentation and Discussion

Presenter: Meghan Hertzler, Xcel Energy
Facilitator: Ron Binz, Public Policy Consulting

Ms. Hertzler presented the draft principles from the Access and Participation Work Group and thanked members of the work group for their contributions. The principles are as follows and can also be viewed under November 22 meeting documents for the Access and Participation Work Group:

1) Data Collection
   - I. Reasons for Customer Data Collection
     - Customer Data is collected to support Primary Purposes, or with the customer's consent to support Secondary Purposes.
   - II. Data Minimization
     - Service providers should only collect Customer Data that is necessary to accomplish a Primary Purpose, or with consent to a Secondary Purpose.

2) Data Use
   - I. Primary and Secondary Purpose
     - Primary Purpose is the use of Account Data or CEUD that is reasonably expected by the customer: 1) to provide service; and 2) including compatible uses in features and services to the customer that do not materially change expectations of customer control and third party data sharing.
     - Secondary Purpose is the use of Account Data and CEUD that is materially different from the Primary Purpose and is not reasonably expected by the customer relative to the transactions or ongoing services provided to the customer by the Service Provider or their contracted agent.

3) Data Retention
   - I. Retention Length for Customer Data
     - Service Providers should retain Customer Data only as long as needed to fulfill the purpose it was collected for, unless they are under a legal obligation to do otherwise.
   - II. Customer Data Disposal
     - Service providers should securely and irreversibly dispose of or de-identify Customer Data once it is reasonably determined by the service provider to be longer necessary to achieve the purposes for which it was collected, unless they are under legal obligation to do otherwise.
   - III. Responsibility for Customer Data Previously Shared with Third Parties
     - Service providers should maintain records identifying what data has been shared previously with third parties, when the sharing occurred, and with whom the data was shared for as long a the data exists in the service providers' systems or as long as legally required.

4) Data Access Rights
   - I. Customer Access
     - Customers have a right of reasonable access to their own Customer Data.
   - II. Third Party Access to Customer Data with Consent
     - Except as specified in Data Access Rights principle III, customer consent is required before the service provider shall provide a third party with access to the customer's Account Data and CEUD.
   - III. Third Part Access to Customer Data without Consent
     - Prior customer consent is not required to disclose Customer Data in the case of:
       - Third parties responding to emergencies that pose imminent threats to life or property;
       - Law enforcement or other legal officials to whom disclosure is authorized or required by law;
       - As directed by Federal or State law, or at the direction of appropriate regulatory authority; or
       - Contracted agents of the service provider supporting a Primary Purpose.
   - IV. Access to Data Other than Customer Data
     - Except as required by law or to support a Primary Purpose, service providers will not share with a third party the customer's: social security number; state or federal issued identification number; financial account number in combination with any security code providing access to the account; consumer report information provided by Equifax, Experian, TransUnion, Social Intelligence or another consumer reporting agency; individually identifiable biometric data; or first name (or initial) and last name in combination with any one of the following: 1) date of birth; 2) mother's maiden name; 3) digitized or other electronic signature; and 4) DNA profile. Such information should be obtained directly from the Consumer.

5) Data Access Methods
   - I. General
     - Methods of providing customer access to Account Data and CEUD should be reasonably convenient, timely, and where appropriate, cost-effective.
   - II. Cost for Customer Data Reports
     - To the extent that a service provider offers a method of data access for data requestors that is different from the method it generally offers to its customers, or not based on commonly used data formats or standards, that service provider may charge a fee, subject to applicable laws and regulations.

III. Costs for Aggregated Data Reports
- The service provider may allow for recovery of costs for Aggregated Data requests that are different from the method or format in which it generally offers aggregated data, represents the fulfillment of multiple requests, or is not based on commonly used data formats or standards.

6) Aggregated Data

I. Access to Aggregated Data
- Data that is aggregated in a manner that limits the likelihood to re-identify a customer may be made available.
- Aggregated Data may be shared via a contract between the service provider and third party that may include language limiting uses of the data, including a requirement to not re-identify customers.
- The service provider may decline a request for Aggregated Data release if fulfilling such a release would cause substantial disruption to the day-to-day activities of its personnel.

II. Requirements for Aggregated Data
- [Tabled pending PNNL research]

III. Aggregated Data Methodologies
- Aggregated Data methodologies should ensure a sufficient number of customers are included in the aggregation to reduce the ability to re-identify a customer.
- Methods by which data can be aggregated should be reviewed every 2 years to account for changes in technology.

IV. Exclusions
- Aggregated Data that contains trade secrets, even when aggregated, may not be released.

Mr. Binz invited participants to provide comments and feedback on the proposed principles:

- Just a quick question on the definition of primary purpose versus secondary purpose. I was curious as to the intent behind defining it based on what the customer would reasonably expect.
  - We have had some discussions about how customers sometimes have their own view of the world. That might differ from what we think is reasonable. As a contracted agent, we are interested in ensuring that what we are doing is a primary purpose. Just trying to think about how in practice a contracted agent would look at the standard and know whether they are following the definition or not of what the customer should reasonably expect.
  - Sure.
- All throughout the principles, I think you hear over and over again the importance of transparency and communicating out to the customer what data is being collected, how it's going to be used, and the areas of the informed consent where it is going to a third-party, what is that data being asked for and

how it is going to be used. The principal cannot get into the detail of what primary purpose is, because that will be different depending on the different service providers. I think you would look to what the service provider communicates to the customer when they collect the data. When you look at it from a rate regulated utility standpoint, oftentimes -- this came up in our workgroup -- we talk about it from the standpoint of what is a regulated service as opposed to a non-regulated service.

- This was drafted with the idea that we use service providers who may not be utilities as well, the idea is, what is being communicated to that customer? What is the reasonable expectation when you have collected the data, and you're going to use it for something that is materially different, you may need to go back to the customer and provide them with notice and depending on the circumstance, obtain consent. Will this the perfect? No. One of the things that makes this space so exciting is that everyone has a different idea about what is private. I would look at this from the standpoint of what was communicated to the customer at the time of the collection, if that helps.
- That makes a lot of sense that you would look to the expectations. You would look to what was provided to the customer at the time of the data collection as well, right?
    - Sure.
    - The questions I raised earlier were addressed by a lot of the good work that your group did. I have a question on access to aggregated data, specifically regarding data aggregated in a manner that limits the likelihood to reidentify. I would imagine there was some discussion around the metric around that. To me, it “limits the likelihood” is a fairly low bar. I was wondering if you could discuss whether or not a higher bar could reasonably be expected to allow for the re identification or something of that nature that would increase the stringency of that.
- We avoided going to a specific metric just based on some of the testimony that has been offered in California that has taken some of those classic data aggregation levels and said they may not really worked to prevent re-identification or to prevent being able to get customer level data. The language that was in here; I'm wanting to say it was modeled after the California language. Chris will have to keep me honest if he still on the phone there. The intent behind it is, without picking a specific formula -- we were not confident we had one we could pick that we could say was a sure one -- however you get there, it has to be reasonable to assume it's going to be protected. You may even want to secure some contract if you have doubts that who you are giving it to will not make efforts to reidentify or try to get at the customer level data. One of the things we were hoping is to maybe expound upon this and provide more detail. By itself, that statement probably doesn't give enough guidance. We were hoping that we would be able to, under this placeholder I have up on the screen, get at the nitty-gritty little bit more. In lieu of not having that, I would be on the side of having prudence around this issue and making the standard a little stronger.
    - My concern is that misapplication in this area probably poses a risk for our interests to encourage smarter development than the standard would improve this.
- My point is that if there is a misstep on privacy and data is somehow misused, perhaps even well-intentioned, but perceived as misused and abuse of the customer information, that that might cause a bigger limitation to smart grid use, than a standard that would require a higher level of metric around how you would treat aggregated data. Is that more clear?
- I think you are really talking about public acceptance and confidence. To the extent that information was reidentified or identified, that undercuts everything that we are trying to do here which was to make sure that the public has reasonable confidence in these practices.
    - Exactly. The item right below that where we talk about aggregated data being shared and the requirement that language limiting the use of that data -- could we consider a statement on the

limitations for subsequent release of that information from the individual party, if I know there are many providers to providers in the sense that the data gets passed down?

- That's a really good comment, and one that maybe we would explore a little bit. In the current principles of data access, we did not put requirements on third parties. When you're talking about aggregation that would be something of an exception. Here you might want an extra level of protection being put out there because you are bypassing consent. As a work group, we looked at this from the standpoint of, we're not controlling the third party. Your point is a valid one.
    - Regarding aggregated data methodologies, we talk about the methodology to ensure a sufficient number of customers, and cognizant of the situation where you have one large customer. The number may be some statement around the type of entities in that aggregated data, non-homogenous data set or something of that nature. You understand the situation I'm concerned with.
- This is where the 15 and 15 rule requires that in your data set, you don't have someone who has greater usage than 15% of the whole. It is a very valid point. Where we struggled was not wanting to choose a winner among aggregation methodologies, and hoping if we had some results that said, here are risks that need to be managed -- of which I think you just identified a risk -- that might be incorporated in another principle. If what we get does not help in that regard, I think that is something that needs to be considered for the workgroup to develop its own kind of risk list.
    - I agree.
- I want to make a follow-up comment related in nature to the ones that Dan was making about aggregated data. He mentioned limiting the likelihood. It seems like a low bar.
- Part of the reason we phrase things the way we have is because of the uncertainty out there. I feel we are trying to figure out what the safe threshold is for aggregated data because it is sort of like antivirus. The more you figure out ways to protect your computer from viruses, it is this ongoing struggle and you have to figure out, is there really an absolute. That is my shorthand way of saying, that's why I think we phrase these discussions regarding aggregated data the way we have. That made me look at one of the principles here in customer data disposal, number two under data retention. We say that service providers should securely dispose of or de-identify customer data once it is determined to no longer be necessary. I think securely and irreversibly disposing of is one thing. Maybe there's some language we can think of coming up with. It seems like we have faced the same uncertainty or at least evolution.
    - How would you know you have securely and irreversibly de-identified customer data if you have just got anonymous individual customer data?
- We are researching ways, and we are so early in determining, could somebody take an anonymous customer data and figure out who it was. If it was particularly unique, perhaps. Instead of being such a low standard, this strikes me as such a high standard to securely and irreversibly de-identify data that I think that might prove to be a challenge. If we can create explanation around what might be considered de-identifying. We cited guidance for de-identification of protected health information. The HIPAA standard. We were trying to keep the principal at a high level that gives guidance as to what that would be, and HIPAA had already seemed to plow that ground. That is one of our references.
    - Maybe there is some language the workgroup can consider in terms of irreversibly de-identifying customer data in light of the technologies and practices available at the time.
- I always rely on the workgroup to create these great edits. I failed you.
    - Point taken.
    - I want to respond. We are stuck in two different worlds here. The one point the principles are trying to get at is, we need to recognize there is some amount of data that can be aggregated anonymously that should be made available without customer consent because there is a low

likelihood of being re-identified. “There is a lot of”, what does it mean? I don't think any of us really know what is a sufficient number of customers. That is kind of in there purposely. People will have different expectations around that area we don't have any metrics or algorithms to determine that today. I think for the short time that is OK. What is sufficient aggregated data to me may not be sufficient aggregated data to you. We really don't have any real way of recommending a particular measure to re-identify a customer. That should not limit the recognition that there should be some amount of data that can be made available without consent. That is one of the reasons that some not covered in our privacy rules, because that is not covered.

- We had a long and very productive conversation about this, so I'm glad you're on the call.
    - This has been way much of my time over the past year.
- He's not talking about the work group, he's talking about his day job.
    - I will inject a question into this. We just heard from EERE, who obtained an anonymized data set to investigate the question of what are the implications of aggregation and de-identification. Where have we gotten on the question of anonymized data, not aggregated, but anonymized? I know we have heard in the past from research institutes who say they need that, certainly utilities themselves need that, and probably other researchers.
- The principles we talked about here do make reference to de-identified data in regards to data retention, and also makes a reference in regard to data aggregation. One of the notes I certainly took from the discussion we had today that we really do not identify what is de-identification. As far as what is the latest, greatest word on that, from what I have seen it, it is still in the camp of the aggregation methods, which is, what can you reasonably do. Part of the challenge is there is so much data out there on individuals that could be overlaid. Even if what you release is reasonably de-identified, are the keys to re-identify and the public domain or part of what the third-party obtaining the data may have within their own data sets.
    - Would it be beyond the scope of this document to spell out what we believe would be de-identified?
- Under HIPA, the first is that a statistician verifies there is very low likelihood. The other option is removing 18 pieces of information. By removing those 18 pieces, date of birth, date of service, you are HIPAA de-identified. There is no such thing as fully de-identified data. There is truly no gold standard in that, but you can lift 18 pieces of data that utilities may have, and if we pull those out, we can say that is what our industry considers to be de-identified.
    - I don't believe it's beyond the scope.
- That's why I took the note. I think we are reluctant to do that until we see how it would be applied to utility data. Even HIPA standard has been crashed. We have seen the stories where people have been able to identify data. I think we memorialize some, we want to have some confidence about whether something like that is going to be measured. So, again, it is something the work group can have a discussion about, identifying a minimum list of things that need to be removed for data and say in addition to that there are other risks. I think that is possible. Not having had that conversation with my cadre of experts, I am not going to be able to tell you how we would accomplish that.
    - One of the things we want to accomplish in this section of the meeting is to give everybody some guidance about what steps are necessary, we were interested in hearing about the project from DOE to see how to stage our VCC with relation to their work.
    - The other input I am interested in hearing, and this audience, this group of participants should be the best at supplying this, what is the state of the art in the sense of, what the demands, requests do you have for the production of aggregated data? Whatever you want to call it.

  - Are we correct in assuming this is becoming a very big deal and requires a lot of careful focus? I have a woman in the room nodding yes. Can you help us understand that? Go to the microphone, please.
- Are people clamoring for this data?
  - Is that correct?
  - The answer is absolutely. Providers are looking to make money off of this data, at least on customer energy usage. You have programs, and you have people looking to control thermostat, appliances within your home, you have appliance manufacturers looking to make appliances smarter. Everybody is clamoring for the data. That is why it is such a big issue. Because so many people with so many opinions and so many reasons for wanting aggregated data, it is a big issue and is something that I think stakeholders can agree needs to be addressed sooner than later because the train is moving and if you do not control it, it might flip over.
  - Do any of the utilities have a story to tell? They are all looking at their shoes.
  - You know, I would say, yes, I work for a utility. We are getting requests for more and more granularity. We have provided for our large areas, kind of at a municipal level, a report on an annual basis. We are seeing that within counties and municipalities, people are looking for more granular reports. For neighborhoods zip codes and census blocks.
- In Minneapolis, we have a green corridor that is being put into place and people want to know how the energy usage goes along that corridor. We see a whole building being a significant demand, as cities are adopting green building ordinances. An important area for conservation and energy efficiency. So I think that is what really drives the discussion of aggregation because you take it from the state or a large city level down to the smaller level, the question is, what is the safe level? At what point do you have to get consent and at what point is it safe to provide the data directly to a third-party?
- As people are looking in smaller and smaller areas, that is where the question comes up. In particular for the commercial and business customers, many times people asked that it be segregated by rate class. You have a lot of residential customers, that is not where the rub comes in but you may have one large customer or a small handful of commercial customers or something like that, as you drill down. Understanding that safe level, that becomes key because even as you are aggregating for a larger geographic area, customers may consider the data to be very sensitive to their bottom line.
  - Anybody else on this topic?
- The city of Philadelphia has mandated customers with multiple, certain size square footage of buildings within the city, aggregated data using the portfolio manager and then reports that in a public way in order to be able to have people shopping for space to rent to know how efficient the buildings are. This data is aggregated to the building level and then it is put in into an index, which a portfolio manager does. But it does not specifically list the energy usage for the tenants or anything like that. It is just an interesting thing because the building owners now have an interest in the energy intensity of their building, so it is kind of a secondary thing. It kind of gets at the question you asked about how interested people are in this data and people are interested in the data. They would report an index. The portfolio manager comes up with it.
- And we have done a project we have completed that automatically feeds data from our manager to the portfolio managers so they can do it automatically rather than having to keep the information in. So it is just another step.
  - Interesting. Anything else? Anybody on the phone lines want to catch Megan before she sits down?
- Hi, I am actually going to respond, Ron, to your request for what is going on in the world. So for the better part of a year, California had been holding meetings, workshops, taking comments, and taking in

proposals on what does aggregated data mean to the regulated utilities in California. So there is a lot of interest. We have heard from a lot of parties that want to get access to usage information and what not. And the basic gist of it is, we have researchers who want to do a lot of fun research to analyze statewide energy policy. I'm sure there are others who want the same thing. How do we get them access to the appropriate level of information?

- We have third parties that want to market directly to rooms of customers that want to understand what the market looks like for their product and services. And then there are other nonprofits that are also interested in this information. So how do we give access to those purposes, which are all beneficial, but in a way that protect customer privacy under the California rules. We have had a difficult discussion over how to do that because we all have an expectation that the customers are expecting us to protect their privacy and act in their interest. So we have two masters to serve.
- There is a lot of interest. We have done a lot of work so far. We have also been lucky enough to have privacy advocates, who have introduced us to a number of computer science researchers at IBM looking at algorithms that can take request for information, personally identifiable information, and then spit out the response in a way that does protect privacy. And the data cubes are not easy, cheap, or seem to be implemented. There is a lot of research to be done on this question to develop algorithms so the privacy can be protected appropriately but it can also be made available to those who are seeking it for legitimate purposes, and I think we are trying to get, people have heard me speak about this, I'm hoping that we can get a decision out by the end of the year or January. That would be helpful to a lot of us. Thank you.
- We may have exhausted this topic for today's purposes; obviously there is more work to do. Megan, did you hear anything that confirms or chases you off of the agenda you were on?
    - No, we knew we would have some work, we being the work group. I think we have a few more pointers as to some of the things we need to do. I know Brandon has taken copious notes and he will come up with an agenda. I do think we were hoping to get some more information that we could use for taking a deeper dive into data aggregation.
    - I'm hearing the need to look at it. I would put a call out generally to the community and say if you have things that you think would be helpful to the work group, go ahead and send them to me.
- My e-mail is on the website. I would be more than happy to give that to the work group as we consider putting some principles out on that space.
    - I do not know if it is active. But there is a link in the forum that was put up or sponsored by the -- was it the privacy group?
- I will go look for that.
    - If you are a member and want to send me a link, that would be great.

Process for Integrating and Compiling Principles; Stewardship and the Future of the VCC

- We are talking about the process of integrating and compiling principals. On the last leadership call, we distinguish between assembling the parts, which is what we did today, and compiling them, a loving reference to old computer programming terms. This was a discussion of an executive committee or parts thereof, thinking that a task force needs to exist to ensure consistency across the sections, to maybe put together a list of final questions, which have now come up after today's discussion. Your thoughts about that proposal and your interest in that. Everybody's giving the thumbs-up.
- What we will do is Eric and Tanya and I will be looking for volunteers for this, we will look at the work group leads to compile the information they got today, and we will put that through a compilation process to get a final principles out. Especially for those of you today who have raised issues, that you want to track, it might be worth your while to join in that group as well.

- The last topic of the day is we are getting close to having a product and in your agenda you will see a series of questions about how this VCC lives, how it will be disseminated and who will be responsible for maintaining and how it might be, what are the guidance, guidelines, if you will, for its adoption. Will it be a living document, able to be revised in future years as needed. So you see that set of questions. Nothing we do today will be final, but we are looking toward the end of the process and we would like to add some ideas from you about the future of the project, the future of the VCC. I do not have specific questions, other than one's the leadership group put together on this agenda.
- We had a decent discussion, several meetings back. I think people are thinking about that. Does anyone have anything to offer right now?
    - Two questions; how will we know when we are done and what sort of consensus do we want to achieve among ourselves in order to say yes, we are done.
- We will make you king for the day. What is the answer to your own question?
    - I was really asking the question.
- When we are exhausted?
    - No. Are we going to ask the folks that are actively participating in this to say that your company approve of this, as your company want to adopt this? What are we looking for? Because when you say how it is going to be released and everything else, at what point do we release it. That is the question I have. When do we know it is OK?
- I am not looking to go until I retire or anything like that. Let me offer a couple of thoughts. I am guessing we are not going to require signers to any document or any individual company. I think the purpose is to offer a relatively low cost shot at having an influence on this process and on the product. I think at some time, I do not know if it is the next meeting, I am sure Eric would like to check this off, some meeting I think we will have a 'speak now or forever hold your peace' kind of call. If there are no serious objections, we will declare a consensus and I think it is up to DOE to publicize the fact this has been agreed, and to some extent you can get into the area of silence means to send, but we have been noisy about the fact this is going on. I know many people who are not involved that know about this process.
- I am glad this is back in the news, all of the stakeholders have the opportunity to come into the room and object and if we do not get objections, we are done. That is my guess. In terms of the rollout, the announcement, the presentation, what kind of parchment paper it is put on, that will be up to DOE, with your guidance.
    - Ron, I thought I would talk about a similar process in that critical consumer issues for them, which is a joint initiative by the association of commissioners and consumer advocates and the Electric Edison Institute. We have, over that time, released two reports, one on grid modernization and energy resources, both of which are sets of principles, and actually the process followed very much which you had indicated, representative of these groups together, in rooms for a day and a half over multiple days. Individuals, and those representatives coming to an agreement, nonbinding on the Association, that is the process that you have outlined leading to DOE.
- I think the bigger question is what next? Because I think that is where the tough part is. You release the report and it is publicized but really what is going to happen to move that forward? That probably is something where individuals here and related to associations they work with, whether they wish to take a role in moving the conversation forward, to take a look at it. Either taking it into conversations in their state commissions, or taking it into conversations more broadly, all of the potential third parties.
- Ultimately what we are trying to do is get people to embrace it on some level. I think that is something, that second stage is the critical thing. I think we can get to the release of the report and then what happens and I think part of that is that persuasion factor to get people involved. And then the third question, people are interested. They like the principles. Do they sign a piece of paper? Do they go

online? What is the way to effectuate adoption or agreement to the principal? That is that third question.

- I'm not sure if that is helpful, but I think in addition to setting out the immediate process, thinking how you move it, move it to those next stages, so it is not a report that gets a press release. I'm not trying to be negative about that. We want to get past that. Those are the questions for all of us.
    - Very well put. I think many of the people in this room have connections to their associations and if you want to justify post hoc what you have been doing, it will be to get a critical mass of your colleagues together to do this. It seems to me if, for example, the utilities in this room are able to hold hands and agreed to jump in at the same time, that will be very helpful. Ditto for half a dozen or more consumer advocate officers saying if you're inclined to endorse it, certainly we would look to the vendor to do the same thing. We obviously will need a good batch of the beginning to make this OK for others to follow.
- We have not talked about this, but I think that's a good point. We are going to need to somehow the evidence someone has actually said they have endorsed this and perhaps at a listing on the way to do that. Thanks. Really good points. I know I asked these questions leading up to this meeting. I will try to suggest a comment rather than more questions.
- I know one of the things we were considering and one of the questions raised is, not having had the benefit of our report from the DOE, wondering, do we release our principles now or do we wait for the study to inform any further revisions and then release it all at one time?
- I think what we heard today was that we have a draft next month that might be ready for publication. That does not seem farther out in terms of our compiler committee. I might suggest that we wait and tried to get the benefit of the information from the report, what benefit there is, before we release the code of conduct to be adopted.
- The other aspect of that is, as was mentioned, the benefit of having many entities jump in the pool and adopt it. I think the more clarity around the principles and the certainty, the more comfortable entities would be adopting without changing. On the other side of that coin, we talked about how there might be, this is early technology, there may be reason to review this and revise it as circumstances change.
- I think we need to struggle with the balance of this being a living document that can be flexible and an environment that is evolving with providing the certainty that an entity would need to say we are going to comply with this. We have to figure out how to do that. I think an update any more frequently than two years is probably a mistake. Something along that scale is what you want to do. We are dealing with eternal verities. They should not change. I think it is clear that the process doe constructed to go through this, the workshops we have been doing in the open work group approach, ensures it is not going to have any hard right or hard left turns after it leaves. This is the way it works. Just looking on the question, see if I have this covered. Anybody on the phone lines one to weigh in on this?
    - No questions.
- Thank you. Anything else for the good of the order on this question?
- Some of you raised the question of what do we need to do to promote this as a group? Seems to me that is a different assignment than what we have been through, so if we can get this closed out and have a product we want, then I think we will reassemble, if only by telephone, to ensure that everybody is working to get the word out, within the bounds of what you might expect to be able to do to get entities to sign on to this, perhaps we can get a boost from regulators, regulator associations, something like that as well to help with that.
    - Just after hearing the discussion around this, do we recommend, similar to pulling together this committee that is going to compile the document into one seamless VCC, should we put together

a group to put together an outline of what might be, how we might move forward to try to answer some of these questions we have been talking about?

- The process or where does it reside?
    - How do we know if somebody has adopted it or not?
- Would it be worthwhile to pull together volunteers to put that together a little bit and then maybe at the next meeting, that is something we put on the table as a proposal rather than open ended like it was today. That might be a way to get past some of this, I think. Any thoughts? Good idea? I do not want to overburden anyone, but I think if folks want to be involved, we can propose that. There might be some folks who can only do one or the other. I think that is what I am thinking, what I heard as far as maybe we are not ready to get into the details on this yet because we do not have anything on the table to react to, so we have an outline of a proposed process that tries to answer some of these questions, and then we can get a response from folks in the next book meeting.
    - I have something to say in terms of process. The phone call meetings are not all that costly when you find places on everybody's calendar. I think the executive team should meet by telephone and either nominate themselves or commit to finding somebody to work on this implementation task force, which will be needed.
- There are a few people, many of you in the room have been active on this. We certainly don't want to overstay our welcome with you, but I think if we take, as you said, the assignment and take it to the group that has formed the executive committee and ask them to create something either themselves or people they will draft into doing it, I think the next meeting should be one in which, unless you disagree, the next meeting of this will be for final adoption.
- We should be able to get everything passed around, all of the cleanups done, all of the emphases shifted in the way we heard about today so that we are only one meeting away from a final product and that same meeting, which adopts the final product, should hear the first report from a group which is thinking about, two things, what the rollout looks like, how subscriptions are induced, and also the answer to the living document questions. I'm seeing some nodding on that proposition.
    - That sounds right to me as far as the next process.
- I think we will probably play it by ear as far as when the next meeting is, depending on how much progress we are making within that implementation group, as you said, as far as getting the final VCC compiled and put together and working out the overlaps or gaps whatever. I guess, what I am saying is, we will play it by ear as far as the next meeting. I think that is the next step to convene the group through a series of conference calls after the Thanksgiving holiday. We can begin that process and hopefully sometime into the New Year, I expect we will be working on this when we do get results of the study and then if there are appropriate things we can incorporate and change higher to finalizing the document, we go ahead and do that. Because of the timing, I think it will work out that way. I can't imagine we are going to rush home and finish this work by January 1, when there are three holidays between now and then. I think the timing is right that we will have some time to incorporate that. Obviously before the next public meeting. That is where we will roll out the final version for consensus adoption. Final thoughts before we adjourn for the day?
    - I just want to say, I have been along for the ride since you held your first group to talk about this. I feel like we have come a long way. When you look at what has been on the screen and all the work that has been done, this has moved a lot of talk, a lot of material and content into very good principles. Yes, we need to be doing some harmonizing, some consistent word use, things like that, but thinking back where you started, I would certainly hope you feel like you are on track because I feel like a lot of work has been accomplished by everyone who has given their time. I just wanted to acknowledge that.

- I appreciate that. I would have to agree. The quality has been very high. It has been satisfying to be part of the process. If you look back over one year ago, when we started this process, we have made a lot of progress. I think we have you to thank for that and volunteer your time and companies to allow me to participate. Hopefully we can finish up and roll it out and declare it a success. Thank you. And the other folks, final thoughts? I'm going to miss you guys. OK, with that, we will consider the meeting adjourned. Thank you, everybody.

Adjourn

The meeting adjourned at approximately 3:00.