# TECHNOLOGICAL CRIME ADVISORY BOARD
## Technical Privacy Subcommittee

**MINUTES OF THE MEETING**

**April 17, 2014 at 1:30 PM**

VIA VIDEO-CONFERENCE
Office of the Attorney General
100 N. Carson Street, Carson City, Nevada 89701
And
Office of the Attorney General
Grant Sawyer Building
555 E. Washington Street, Suite 3315, Las Vegas, Nevada 89101

1. **Call to Order and Roll Call:** The meeting was called to order by the Chair, Hal Berghel.

**Present:** Hal Berghel, Chair; Stephen Bates; Dennis Cobb; James Earl; James Elste; Allen Lichtenstein; Ira Victor.
**Absent:** None.

**Staff Members Present:** Brett Kandt, Special Deputy Attorney General and Executive Director, Technological Crime Advisory Board.

**Others Present:** None.

2. **Public Comment.** The Chair asked if there were any public comments from Carson City or Las Vegas. Hearing none, the next item on the agenda was called.

3. **Chair's Welcome.** (Chair)
Hal Berghel thanked the members for attending the third meeting .and appreciate that you have willing agreed to participate in this important subcommittee activity.

4. **Discussion and possible action on approval of December 6, 2013, meeting minutes**. Motion made for approval of Minutes; all in favor; motion carried.

5. **Discussion and possible action on approval of February 21, 2014, meeting minutes.** Motion made for approval of Minutes; all in favor; motion carried.

6. **Report from Allen Lichtenstein on project to identify all Nevada Revised Statutes that affect privacy rights. (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

DRAFT

Mr. Lichtenstein:
We are a little behind in getting the information. We are using volunteer interns and have had some turnover. We may have to wait until the next meeting although you just showed me where a lot of this work has been done. I would like to look at this and report back in the next week if that would be OK.

Mr. Berghel:
We will carry over Item 6 to the next meeting.

7. **Report from James Elste on request for assistance from Electronic Frontier Foundation to develop legislation to expand online privacy rights. (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

Mr. Elste:
I am pleased to report that there was a good interaction with the folks at EFF. Jim Earl and I had a conversation this morning Lee Tien and two other representatives of EFF. One, David Greene, who specializes in First Amendment law and Adi Kamdar who I believe, is responsible for monitoring EFF's state legislative agenda. They all were enthusiastic about the work we're doing on the Privacy Subcommittee, very interested in engaging with us and supporting the work we're doing. With the caveat that EFF does not necessarily automatically endorse things - they chart their own destiny. Their willingness to share information with us, to put us in contact with individuals that might be helpful in our pursuits and generally support the work we're doing by not only contributing that information but also helping us shape topics that we should be considering.

We had a very interesting discussion around some of the privacy priorities that EFF is looking at. I would like to share those four or five items because I think they will help shape our future agenda and some future topics that we might discuss. Lee Tien is a senior staff attorney at EFF and has been there since 2000. He has been intimately involved with EFF's efforts on both the federal and state level. He has been involved in everything privacy related. I believe he is an excellent guy to be able to tap into.

The priorities that they are looking at have some very interesting implications for our work. One to the top priorities and hottest topics right now is the question of drones and how drones may be used from a surveillance perspective. Given Nevada's role in the drone program being one of the 6 states chosen to be part of that, I think it might be an excellent issue for us to take up as a privacy group to try to explore what some of the privacy implications are with the drones.

Mr. Earl:
One of the things that we didn't talk about with them but which they made a point of distinguishing was public sector use of drones and private sector use of drones. It was clear in their analysis that there were two different drone regimes that they felt needed to be addressed separately.

Mr. Elste:
Second issue I think we have already broached here which is the automated license plate readers and implications for privacy with regards to that technology. Lee spoke at length about his work with location tracking and cell phone searches which is another interesting area of exploration from a privacy perspective. How cell phones are allowed to be searched, how location information, in particular, is collected and used.

The other two are interesting and might be worth consideration but implications for biometrics and how biometrics might be implicated in privacy considerations. Finally, he spoke about more of what he called a process area which is transparency and particularly, transparency with regards to law enforcement organizations. Apparently, in California there is a concern about the acquisition of technology like drone technology by law enforcement organizations without any sort of visibility that those types of acquisitions are being made.

Those topics and priorities are what EFF are focused on. I think they have certain relevance for us as an organization focused on privacy here, in Nevada. The good news is the EFF is a very willing and a staunch supporter for the work that we are doing here.

Mr. Kandt:
Can you please clarify the names on the two gentlemen you mentioned?

Mr. Elste:
David Greene – one of the staff attorneys focused on the First Amendment issues.
Adi Kamdar – legislative agenda at the state level.

Mr. Berghel:
Do you have available links to the EFF that you might send me so that I could post a note?

Mr. Elste:
Yes, I'd be happy to send you some links to EFF. They mentioned some blog posts. Later, in the meeting today, they provide us with some interesting commentary on the shield law which is another agenda item. They offered to put us in touch with an individual who has been actively involved in shield law at a federal level. What I am hoping is that we've opened the channels of communication and start to be able to get to exchange information; get links; get input on things and that we will perpetuate that and evolve that communication.

Mr. Berghel:
Brett, I have a question – is it possible to invite some of these interesting people to the TCAB Board meeting?

Mr. Kandt:
I think if we identified who you want to invite and then I can explore some possible funding opportunities. I think if you are talking about a single individual, I can find the money. If you are talking about multiple, it may be a little more of a challenge.

Mr. Berghel:
I think we can find several candidates that would be useful to us both in TCAB and Privacy Subcommittee. We'll get back to you shortly with possible recommendations and then you can discuss it with General Masto or your budget officer, whoever is appropriate.

Wonderful! Thank you. Our next agenda item was suggested by Stephen Bates and it has to do with the Utah License Plate Reader System and that is currently in the courts, as I understand, in Utah. Can you give us an update?

8. **Report from Stephen Bates on Utah Automatic License Plate Reader System Act, Utah Code § 41-6a-2001 to § 41-6z-2006, and pending litigation in *Digital Recognition Network v. Herbert.* (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

Mr. Bates:
I don't know that anything more has happened in Utah but the lawsuit has been filed making it a First Amendment violation to tell these companies that they can't continue photographing and marketing the information. These companies are selling information to government agencies and in some cases; they are giving information to government agencies. They are also selling the devices to car repossession companies and insurance companies. There was a report earlier this year that this technology principally is used by government, including large part, the retention of records. It seems like a very important issue to address but it's easily evaded as long as the private companies are amassing the information without some sort of regulation. In the case of many of them, sharing it freely with law enforcement which is certainly their right.

It is, as was mentioned at our last meeting, in some ways, like standing there with a digital phone and taking a picture. At some point, the difference of degree becomes a difference in kind. A patrol car with one of these devices on it will capture, on average, 6,000 plates per day. One of the companies, MVTracks, has photos and location information for a majority of registered automobiles in the United States. Digital Recognition Network has a national network of 150 affiliates and has 700 million data points on American cars and their whereabouts. There is no limitation on how long they can keep the information. At present, Utah has a law against it. Arkansas, New Hampshire, Vermont and, Maine have laws restricting use by private entities and public entities use of this technology. The companies who make it are understandably alarmed about that and have filed suit in Utah. Apparently, 15 or 20 states are considering legislation on this because it is becoming a hot topic. In terms of law

enforcement, different states and different entities have different standards on retention. The Ohio Highway Patrol deletes something instantly if there's no match with a missing car. Others keep it for five years or longer. Others share it outside the law enforcement agency right away to DHS or anywhere else.

The last issue that is mentioned in the ACLU is it would be nice to have restrictions on what's done with this information, how long it is kept but the ACLU also suggests it would also be helpful for individuals to be able to send in a request and find out what is on themselves and their vehicles in the database. Also to have these public entities required to keep records and make records publicly available of what they have, how long they keep it, and with whom they share it.

I would be interested in looking more at the private sector side which I think is an important element. Allen may know more about the public sector side of law enforcement agencies and what they are doing with this license plate information.

Mr. Lichtenstein:
It's easier to create limits on public agencies. Public agencies have their own privacy concerns and when you say "people can check", there is nothing to force a private agency to give out that information and nothing to prevent that private agency from selling that information. It's easier to create limits and create sunset provisions whether or not they will be adhered to or not. Within a public agency, they have to justify why they are doing it and the public response is wary about keeping the information forever.

Private agencies are a much stricter matter. You can run into a problem that we have run into in the public records law where public records are obtained through a third party and therefore, it's a private party, this will no longer apply.

And how to you peddle a constitutional law that prohibits people from maintaining information that they legally got. The private is much more of an issue and keeping the public agencies from storing that information with private agencies is another issue that we should pay some attention to.

Mr. Bates:
It's something I'd like to look into more and talk to the EFF people who are active on that. As I said, I think we most interested with public agencies, law enforcement but it seems that even the agents of law enforcement can just pick up the phone and call the repo company and check that data base and find whatever they'd like to. I'd like to look at the laws that have been enacted in these five states and see what is under consideration elsewhere and talk about Constitutional issues and what is involved in regulating private companies.

[Group discussion inaudible.]

DRAFT

Mr. Berghel:
I have a question - you are all aware of Google Earth. When I first subscribed to that service back in the 90's, it was called Keyhole Earthviewer. One of the issues that they found when they drilled down to the street view had to do with the license plates and as we all know, about 6 or 7 years ago, they started dithering them. The question is – Google didn't do that voluntarily, I assure you they were pressured into it by lawyers someplace. Where did the pressure come from? What were the issues involved? How does that relate to the legal situation with license plate readers in Utah?

Mr. Lichtenstein:
It's up in the air; it's one of the things that we will be seeing more and more of in terms of legal squabbles. Are they considered an agent of the government or are they doing this on their own? To the government, they'd be a customer, among many different customers in which case you don't have government action and therefore, you much less opportunity for oversight and transparency.

Mr. Berghel:
I don't know why Google Earth changed that. It was changed when Street View was introduced.

Mr. Victor:
To my recollection, what happened with Google was a combination of bad publicity and concerns of litigation and concerns over legislation at different parts of the world. My recollection is that Google sort of slowly went into those photographs and started changing them but I don't think it was one single element that caused them to start to blur out items in it. It would be a very interesting legal research question. I don't think it was one item.

Mr. Berghel:
We had a corollary to that with some of these anonymizing email services with Lesson?? Was issued the subpoena by the FBI for Blogabid?? Many of the other anonymizing services just voluntarily closed because they could see the handwriting on the wall. As I understand what you are saying, Ira, that may have been going through the General Counsel's mind at Google. They could see that this was going to be a big hassle and it was just better to take a swerve around the whole issue. Is that what you are saying?

Mr. Victor:
You seem to suggest that Google was proactive about it. My observation of Google is that it is very reactive so they would get a spate of bad publicity and then they would react to it. Or, there would be some legislative rumblings and they would react to that. Or, litigation. There are some black and white cases, this is not fuzzy. For example, when it was revealed that the Google Street View cars were capturing Wi Fi traffic and capturing the names of access points, the content of the messages within – they were sniffing the traffic and capturing the information of people that were on a Wi Fi access point that was within the street view range when that car came by. They got caught with

their hand in the cookie jar because they said “no, we don’t capture any of this but somehow, some of the traffic got analyzed that Google Street View had and they said “you guys are capturing clear text information and that includes a lot of confidential data” so then they reacted and said “yeah, we’ll turn that off on the street view cars”. But they didn’t do it until they were shamed.

Mr. Berghel:
That is my recollection as well, Ira. The specific instance and defining moment was when they were caught with use ID’s and passwords from wireless access points. They represented a significant percentage of the global wireless access points out there.

I’m thinking of the license plate reader question, and was wondering is raising a request for an agenda item for our next meeting to actually have a vote and agree to start formalizing some sort of language around a bill for this appropriate? Reading the Utah statute and recognizing the kind of information that is being shared in our discussion, it seems to me that having no law on the books regarding these license plate readers and considering that this is top priority as articulated by EFF today and all of the different implications that it makes sense for us to say this may well be something we should take as an action to start crafting a similar law.

Stephen, I recognize you are going to do some more research and work with Allen to really ferret out what that law might look like but agreeing that you may well pursue that seems to be an interesting action item for us in the next meeting.

Mr. Kandt:
I think as long as the Chair is willing to have that included as an agenda item for the next meeting, I will work with the Chair to formulate the agenda for the next meeting and we can put that as an action item it it’s the Chair’s pleasure.

Mr. Berghel:
I think we can do that by simply rolling over action Item 8 and maybe fleshing out a joint proposal from Stephen and Allen and see where that goes?

Mr. Earl:
One additional thing I was going to say for Agenda Item 17, the committee comments. I think it’s appropriate here. The other thing we spend a fair amount of time with EFF on this morning was answering some of their questions about the way in which the Tech Crime Advisory Boards operate and the way in which the Subcommittee operates. They were particularly interested in knowing where these bodies operated in public meetings or not. The other question was whether their discussions with Jim Elste and me had to be disclosed – whether there was a legal requirement that we do so. I gave them the brief 10,000-foot view on Nevada Public Meeting Law and how both the Tech Crime Advisory Board and the Subcommittee operate pursuant to open meeting law and told them that we have had members of the public attend the Subcommittee meetings in the past and had made presentations or public statements during the agenda item. I went on to say that since Jim Elste and I do not constitute a majority of

the Subcommittee, the threshold of Nevada Public Meeting Law was not tripped and so, there was not a legal requirement on us to disclose an ex-parte communications. That opens the question as to whether we would want to invite them to attend electronically or not but it's clear they were interested in getting a little better understanding as to the legal circumstances that would surround any of their participation or indeed, the actions of this Subcommittee or the Tech Crime Advisory Board, itself.

Mr. Berghel:
Thank you, Jim, for the clarification. Stephen and Allen and Jim Elste work with the EFF on other matters anyway from the Chair's perspective, I would encourage you to continue your discussions and so long as you don't constitute a quorum, go as far as you can along these lines.

Any other comments on the Utah Automatic License Plate Reader? We will leave that until next meeting and move to Ira's proposal regarding full disclosure.

**9. Report from Ira Victor on proposed legislation requiring full disclosure when metadata is captured and retained by government entities (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

Mr. Victor:
It was an interesting research project I tried to find legislation on metadata regarding surveillance cameras. I kept running into the license plate issue. Search after search after search brought me back to the license plate issue and Stephen Bates did a great job. I have a lot of information here that is very redundant to what you found about Utah and Arkansas because so much of it pointed to that. I won't go over that because much of it is redundant and comes from the ACLU national which is not doing a lot of work on this. Everybody that is talking about the topics of surveillance and metadata, many of them are linking back to this very issue about license plate readers. Mr. Chairman, just for the record, I'll send you a link to this so it can go up on your website. It is a very good breakdown that the ACLU did of last year, state by state, what each state is doing regarding license plate surveillance.

I really drilled down hard to find anything on metadata and surveillance cameras. There are a few things about public surveillance cameras, not that much. Nothing about private surveillance cameras – I could not find any references to any material there. I don't know if that means that it is very deeply buried or there just isn't any. Isn't any model legislation out there about this but it was difficult.

One more sidebar, interestingly enough, I pulled this article down from the ACLU that goes state by state a number of weeks ago. Just this week, posted at watchdog.org which is the Franklin Public Policy Center out of DC and they have a very in depth article that got circulated around the web. Who's Watching Me police took photos of my license plates. This popped up on an alert I set up and then everyone was linking to this story this week.

I think it's an indication, unscientific, but still interesting indication that people have a lot of concern about the license plate issue. That might be one from a political standpoint that we can get a lot of support around tackling the license plate surveillance issue. If there is a way for us and I don't think we'll know this until we drill down into it, if there's a way we can start to encompass some of the issues about the collection and long-term storage of metadata and about surveillance cameras in general. It probably would be smart to do something with license plate reading because that has people very concerned. Questions?

Mr. Elste:
We have quite a few different mechanisms for collecting data that is potentially of deep concern when it comes to individual privacy and civil liberties, tracking of location, tracking of people's activities – our cellphones, the way we use certain pieces of technology, things like the license plate readers, all of these essentially create a data source and then the disturbing part of the question is not so much the collection of that data, it's the aggregation and use of that data, the interpretation of that data. If you look at things look at things like Dr. Sandy Pentland's work at MIT, you can, with that data and a certain amount of analysis, determine more about an individual than the data itself tells you.

It seems to me that part of this is a question of framing our discussion around not the instrument, the things like the license plate collector but really the use of the data, the fact that data aggregation, data analysis and then, its privacy locations are the heart of the issue. In my mind, it's a question of framing those into two pieces. It's the "what are the mechanisms that are used for collection that we are concerned about?" – is it video surveillance cameras, it is license plate readers, is it cellphone metadata, is it GPS data from your cellphone, things like that. Then how do we actually get our heads wrapped around and potentially develop legislation that helps moderate how aggregated data is analyzed and used? Once you solve the latter problem, the rest of the mechanisms become somewhat irrelevant. My question to you, Ira, is, besides being stuck in the channel of license plate readers because of the search results, did you find anything that indicated more about uses of the data, the potential downsides of privacy implications of the use of data, or some of work and I'm happy to point you in the direction of Sandy's work because it's really interesting – the types of things they are able to define from this data.

Mr. Victor:
The short answer is yes, I was able to see more although I couldn't find any model legislation. There are lots of grassroots organizations that are very concerned about the general surveillance issues. One that comes to mind is in Oakland. It's an Oakland working group of citizens that are concerned about surveillance by law enforcement in general. I am familiar actually, Jim, the way I would phrase what you said is we've got organizations that can take a big data approach, take all these different data sources and start to reverse identify people. You don't even know who the person is but you

DRAFT

can take the metadata and say “I’m pretty sure that’s who this person is”. This is where they work.

In the article that appeared, my alert from this week, it’s someone tracking them via surveillance going to church which brings up First Amendment issues. There is a general concern about surveillance in general and I think it’s very intriguing to try to tackle that from the perspective of, let’s call it, big metadata. I agree with you, if we tackle the issue of the storage of this data and how long it can be stored, then we start to address the concerns that the citizens have about where this could go.

Mr. Kandt:
I know you’ve talked about two different approaches – 1) the prohibition or regulation approach and then 2) the transparency/disclosure approach. When you are talking about legislation, you could consider one or the other, even if you don’t go to the prohibition or regulation approach, you’d still consider the disclosure/transparency approach.

Mr. Victor:
That is an excellent observation from my perspective; it’s what you focus that either prohibition or transparency on. The possession and use of a license plate reader seems to me to be secondary to the transparency and/or prohibition on how you use the data collected from the license plate reader. As we go down this trail, I suspect there will be some interesting discussions about where we actually point the legislation.

Mr. ??
Mr. Chairman, if I may amplify that – there was legislation two sessions ago that I discovered in doing some research here in Nevada, that would have made it illegal for anyone to grab someone’s credentials over the airwaves. I read that legislation and said wait a minute, we’ve got the data security conferences blackout at DEFCON CEIC on visual forensics last month in Las Vegas and we could be criminalizing when a researcher demonstrates something at one of those conferences that shows vulnerability that act in itself could trigger a legal consequence for the researcher. I’ve worked with Lee Tien to get some guidance on where to go with this. Hopefully, that legislation was defeated. Infoguard actually opposed that and that part of the legislation was changed to reflect research.

Mr. Earl:
If my recollection is right, there was a research exception was put into that.

Mr. ??
It had to do with intent – research and intent – researchers could scan your ID at the conference and then delete everything. The intent was to show research not to steal your identity. It wasn’t defeated, it was just changed.

Mr. Kandt:
When you get into issues of intent, that can create problems as well.

Mr. ??
The point I am trying to make is the actual hardware that collected that data – we don't want to make that the criminal possession. It's how one uses it and uses the data that matters more than the actual device itself for software.

Mr. Cobb:
I go for walks with my camera and take pictures in my neighborhood so my computer contains an enormous number of license plates from the area. The Los Angeles County Sheriff just last week put up a website encouraging people that if they have what they believe are evidentiary videos or photographs they can send them to this website. We need to create a law that everyone that thought they were doing something good by sending in this data but not erasing it from their phone could be protected.

Mr. Elste:
You don't want to throw the baby out with the bathwater. There are legitimate uses for something like a license plate reader that are genuinely beneficial uses so you don't want to make law that prohibits the use of technology for beneficial purposes. Ideally, is produce laws that prevent the use of technology for malicious or otherwise detrimental purposes. That's really the hard part.

Mr. Berghel:
Very good discussion; I look forward to continuing this at future meetings. I have a general question that I would like to direct to the attorneys of the group. In an earlier life, I used to work with a multimedia company and when we did our shoots, especially in New York City, we were required to get waivers for names and the likenesses that included people, buildings. What was it about that that distinguishes it from the license plate readers?

My perception of it is commercial use of image afterwards. Allen mentioned earlier that if you are in public place, you don't have a right to privacy. If someone takes your photograph, that's not against the law. If they take your photograph and use it commercially to advertise, sell, and do other things, then there are civil laws that protect against your image being used without your permission.

How is that not applicable to the private companies that harvest license plate information?

Mr. Lichtenstein:
Every law of publicity that I've ever seen including Nevada's limits it to someone's likeness or image. I've never seen one that said anything about license plates.

Mr. Berghel:
That's an interesting point though because your license plate is arguably unique to your vehicle and whatever registration attaches to that. If I take a picture of it on one of my walks around my neighborhood but now I commercialize it by selling it to someone who

aggregates license plate data and analyzes it for skip tracing or whatever. It's interesting because it almost although it's not an image of you, it's almost the same kind of thing would apply.

I am going to suggest that indirectly this is on our agenda under Item No. 16 so if we can hold off, we can return to this.

**10. Discussion and possible action on proposed amendment to the Nevada Constitution establishing a right to privacy**.

Mr. Berghel:
This was a general issue that Allen brought up two meetings ago. What would actually be involved in getting privacy in the constitution for the State of Nevada, much like California, has?

Mr. Lichtenstein:
I did contact certain powerful legislators and one in particular, said "You write it, I'll introduce it." If we want to put in a request for a constitutional amendment that would mirror California or could be our own simply saying that there is a right to privacy as in general proposition, we can at least introduce it and probably get a hearing on it.

Mr. Berghel:
I'd like to get some feedback from the rest of the attorneys of the Subcommittee about this. This doesn't take much. In Article 1, Section 1 of the California Constitution, it is basically what we have except privacy is included at the end. There's not an awful lot of wordsmithing required for this. Is this something that is viable in the State of Nevada at this date and time?

Mr. Bates:
I wonder if anyone knows what the effect of the California language is, if this created substantial protection? It seems like this sort of thing that could be introduced by legislator or the public without much idea of what's going to happen. The right of privacy sounds great to all of us – it would be interesting to see how often it has been cited in California legal proceedings.

Mr. Lichtenstein
My thought is the protection of privacy that exists within the States come from either specific statutes or from common law in terms of Nevada Supreme Court cases. To me, having just as I practice as a lawyer who deals with some of these things, being able to cite Nevada Constitution or Article 1, Section whatever it might be, I think it also informs discussions on legislation that come up that Nevada has recently created a particular section of the Constitution that verifies the right of privacy which means that it is something that has enough gravitas to it that it might sway some legislation.

DRAFT

Mr. Berghel:
With privacy in the constitution, the State of California gave a lot of impetus behind legislation such as the Right to Know bill that was defeated in the last legislature and the argument there was you see privacy is in the constitution so California residents have the right to know. It took the corporate interests quite a bit of effort to defeat that bill so I think that speaks to what Allen is saying here that is does give some political capital to the rights of the citizens to have privacy.

Mr. Kandt:
I was going to mention that there is extensive case law on the right of privacy that has been determined to exist under the U.S. Constitution. Looking at the fact that California has an express right delineated in its state constitution, Nevada doesn't. Whether anybody was aware of case law out of California in which that express, explicit right to privacy in the California Constitution had been the basis for the California courts making some determination in the favor of their citizens that our citizens lack due to the absence of an express, explicit right to privacy in the Nevada Constitution.

Mr. Berghel:
Good question. I would refer you to the California Right to Know Law which is on my privacy notes webpage. I have a pretty good idea of what kind of momentum it provided the legislature just by reading the draft legislation. Jim Earl, do you have any thoughts about this – you worked with the legislators for a while.

Mr. Earl:
My observation is perhaps simply a rephrasing some of the discussion we've already had. Were Nevada to place just a few words in the Nevada Constitution as you suggested, establishing constitutional right to privacy, I think that there would be a move by diverse groups to flush out that constitutional right of privacy and additional legislation. Whether it's a good thing or bad thing, obviously, it depends on your point of view when you look at a particular piece of proposed legislation. Clearly, this would embolden some groups which I, myself, would personally have to identify as fringe groups that would seek to establish a right of privacy in such a way as to overcome the operation of both state and federal laws. If you put that aside, I think the most likely occurrence I would see is by putting a few choice words in the Nevada Constitution would be an invitation for further discussion as to what that meant. Then, at some later stage, the consideration of additional statutes that would seek to enlarge or delineate what a constitutional right of privacy really meant.

Mr. Elste:
I think the notion of adding privacy to the constitution is a good one. I think it's an interesting question that you hear in privacy circles at a federal level because privacy as a term does not exist in the U.S Constitution. The thing that I haven't heard anyone mention which I'll throw out there for people's attention is that the right to privacy has been defined in the UU. Charter of Human Rights which was developed in the 1950's in which the U.S. is already a signatory on. We have both with California's Constitution and the U.N. Charter of Human Rights, references that we can use for shaping our own

constitutional amendment to bring privacy into the Nevada Constitution. That being said, I think it does a couple of things for us: First, it raises the visibility of privacy and helps us in debates in support for legislation that is privacy enhancing. That's the benefit. The downside is, as Jim just pointed out, is that the interpretation of the term "right to privacy" is not a very well defined interpretation. We will see an interesting struggle around how to frame the discussion on what "privacy" actually means. At the end of the day, what I think it allows us to do is establish privacy overtly in the constitution and use it referentially as we pursue privacy legislation that address issues that are way more complicated than simple questions of is it a privacy issue or not.

Mr. Kandt:
One other possible ramification of actually expressly providing for right of privacy in the Nevada Constitution is our State Supreme Court has routinely held that certain rights that are expressly embodied in both the State and the federal constitutions, they have interpreted more broadly and more extensively under the Nevada Constitution. For instance, the Fourth Amendment Right – protection against unreasonable searches and seizures – our State Supreme Court has interpreted that more broadly to extend more protections to Nevada citizens under the Nevada Constitution than the U.S. Constitution as been interpreted by the U.S. Supreme Court.

Mr. Lichtenstein:
The word "privacy" does not appear in the federal constitution so therefore, we can't really make that kind of comparison. The U.S Supreme Court said it exists by the occasion and various other kinds of amendments. It's always been kind of a sticking point for those who are textual literalists. If it doesn't say it, it doesn't say it. Here, I don't think we'll have our Supreme Court comparing our rights if this thing ever gets through to language that doesn't appear in the federal system which I think makes it even more important to actually have it in writing.

Mr. Berghel:
I agree and by putting it actually in the Nevada Constitution, at the end of Article 1, Section 1, I think it sends notice to people that there's a higher standard they must conform to if you are going to start making inroads privacy and that goes in and of itself, is worthy of some of our attention. California demonstrated that.

In the absence of specific civil rights prosecutable laws in the State of Nevada, wouldn't it just affect Nevada government agencies? So much concern was expressed earlier about the privatization of this kind of thing.

Mr. Lichtenstein:
Technically, yes, just like the first Amendment doesn't prevent your boss telling you not to speak in those circumstances and certainly not yourselves. I think by stating that as a general principle, it gives support to possible legislation that may not cut back on the access kind of thing, at least put some limitations on sharing information and storage. And the other thing is, even if it doesn't pass, I think just having it debated in the legislature or in the newspaper may bring it to light and bring it to public discussion.

Some of the other issues we are talking about that will be affected by it is also something to think about.

Mr. Berghel:
The discussion itself will be worthwhile if the legislation isn't successful.

Is there a consensus on our part that we would like to see a first draft and how we might include privacy in the constitution for the next meeting?

Mr. Elste:
I would ask the same way we did earlier for an agenda item in our next meeting to take that up as an action item.

Mr. Berghel:
We will do that and roll this over and again, could I ask the attorneys, Jim Earl, Allen and Steve, to work together and create a draft for us to look at for the next meeting.

Mr. Cobb:
I have been informed that we can take action on this item right now if we wanted to have a motion on pursuing language for a constitutional amendment, we can agree to do that.

Mr. Berghel:
I'll consider it moved; do we have a second? Dennis Cobb seconds it.
All in favor; none opposed; we will proceed with that motion.

**11. Discussion and possible action on proposed revisions to the State of Nevada Online Privacy Policy (http://nv.gov/privacy-policy/). (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

Mr. Berghel;
This is Dennis's item.

Mr. Cobb:
It was on the idea of should Nevada to have some specific procedures for how you handle, dispose of, transfer different categories information because it's multi-faceted and an enormously wide spread topic to try to make rules on information and it seems to facilitate progress if you can categorize it in some way.

One category is information that in and of itself is not particularly damaging but combined with other widely available information, it could be harmful. Then you have information that isn't particularly harmful but is proprietary because of its business secrets or trade secrets or has commercial value. There is no standard framework for how this information would be handled so the policies that existed in one agency for law enforcement would have no corollary necessarily in the other agency that you need to

share something with. My intention wasn't that anybody must use it but to provide sort of a best practices framework within the State of Nevada private and public entities can use.

Mr. Lichtenstein:
In looking through this, I'm not sure that we can come up with something that doesn't throw out the baby with the bathwater. Looking at the different tiers, Tier 3, I think about the discussion we had probably 20 minutes ago about storing information and accessibility and I can see so much information "Oh that's Tier 3, that's not going to really affect anybody" so it may have the unintended consequence of covering a multitude of sins.

Mr. Berghel:
What it was meant to do was allow a common understanding so you could have a conversation before sharing information.

Mr. Lichtenstein:
This also, in some ways, tracks the government's classified information system which we know what makes something classified may be embarrassing or be classified for no reason at all.

Mr. Berghel:
It was only to facilitate conversations with the parties who wanted to share information with each other.

Mr. Elste:
I think Dennis, as a security guy, I really like the notion of the tiered classification model for information. I've used them in many applications in many roles and it's a helpful tool from a security perspective that helps categorize types of information. The observation I would share with you is that with respect to privacy particularly, that way I've always described the difference between privacy and security is that privacy tells you what needs to be protected, it gives you a sense of why that information is valuable and requires protection or special treatment as "being private or privacy related information.

The security role is to define how you protect it and it includes things like classification schemes, technology like encryption, authentication, etc. While I think this is a really useful taxonomy and I definitely sympathize that there isn't a really good taxonomy in existence currently for state agencies to exchange information, my sense is, one, it doesn't help us from a privacy perspective to create a taxonomy around the treatment of that information, it seems to me to be more of a security exercise to define that taxonomy. Second for an existing agency, I think I mentioned that the State Information Security Officer and Office of Information Security probably have the best mandate for establishing that as a statewide policy. They can define security policy that policy can be applied to all state agencies. More important than that is certain agencies may have a requirement for a different type of taxonomy or a different level within those taxonomies. I wouldn't necessarily think that advocating for a single meta taxonomy

might be the best way. All of that leads me to this conclusion, Dennis, great work, good security practices, let's put this on the Office of Information Security to take up as a responsibility and try to move that forward. Then focus specifically on the sort of what we think privacy-wise needs to be protected.

Maybe that's what we need ultimately is the kind of Rosetta stone classification schemes. It will translate classification schemes from one agency to the next.

Mr. Berghel:
It makes good sense to me.

**12. Discussion and possible action on proposed legislation to expand the news shield privilege under NRS 49.275 to address gaps created by technology.**

Mr. Berghel:
Next is the proposed revision of the News Shield Law that was handled by Allen and Stephen.

Mr. Bates:
In some points, it is like the license plate reader issue in that it seems to be really timely and maybe more than I expected in the case of this. The Media Law Resource Center has a model shield law they had a lot of suggestions for this but have said we should work together in the weeks to come and try to come up with something that everyone could benefit from. I talked with Barry Smith from the Nevada Press Association. We exchanged emails. He had some good suggestions.

Mr. Berghel:
Allen, do you have anything to add to that?

Mr. Lichtenstein:
I kind of agree. We have one of the stronger News Shield Laws of any place that I'm aware. There is kind of "if it ain't broke, don't break it" feeling.

Mr. ??
I would like to add some language that speaks of through any medium now in existence or exists in the future, to address when you have this new media that pop up so that way it kind of covers it. The other question I have is on number 5 and I think that people do have this question of if a subpoena is issued.

Mr. Berghel:
In the interest of time, it's obvious we are going to carry this over. Does anyone in the North have any input for Allen and Stephen on the Shield Law?

Mr. Elste:
I wanted to share some of the feedback Jim Earl and I got from David and the folks at EFF this morning because we had some time on the call to have a discussion about the

Shield Law. I found their comments rather informative. The first thing that they said and I think you should take this to heart was that this is one of the "more rock solid" laws that they have seen. They have been looking at news shield laws across the country so I think that speaks very well the language that Stephen and Allen have developed. They told us that they looked for certain things in Shield Laws and three of the things they looked for were really protection of the journalistic sources, like the identity of sources, the documentary information that they use to produce a journalistic output, like notes, photos, etc., so making sure that our language is expansive enough to cover not just the product that they produce but also all of the material that goes into producing that product. The third thing was the eye-witness observations that they collected in the form of developing that journalistic output.

One of probably the most important pieces of feedback and one that I think will bear some discussion for our group is that they look at the type of information that is covered and who does that apply to. From EFF's perspective, it is the functional definition of journalism that's more important than a status definition of journalism. I believe what we have in the current language is you have to be a certain type of journalist to be covered as opposed to looking strictly speaking at the act of journalism, the function of creating or otherwise producing journalistic output. We may want to consider looking at a way to functionally define journalism as opposed to what is currently a series of labels as if you are one of these, then you're a journalist. Part of that is encompassing non sort of news-related journalist and folks who are for instance, a book author who may be doing investigative journalism of a sort to produce a book that will not be regularly published or meet that regularity requirement. I think that one really resonated for me because an unpublished author who is doing investigative journalism or producing a book that is using investigative techniques may well need the same sort of protection. Those were the primary elements of feedback received.

Mr. Earl:
Essentially, the position we took after EFF laid out its functionality preference was to say, OK, I can kind of understand what you mean conceptually where you would like to define the scope of application based on function rather than on definitions and this extends to a protected class which is described this way for this list of protected things. We went on to say that's fine, if we understand that conceptually, can you give us some examples of the type of functional definitions that you think we might want to consider substituting for the ones that exist right now. My recollection is that they were going to provide Jim Elste with some examples. As soon as that happens, my suggestion would be Jim automatically shares with the Chair and the Chair considers disseminating it to Committee Members.

Mr. Elste:
Happy to do so.

Barry Smith:
I am Director of the Nevada Press Association and would like it on the record that I am here and willing to help and answer any questions and be of assistance however I can.

Mr. Berghel:
Thank you. You are in contact with him I take it, Stephen? Do you have enough to proceed with your next revision? I'm interested in looking at how different states address it. We'll carry this over for the next meeting.

**13. Discussion and possible action on proposed amendments to NRS 205.473-.513, *inclusive*, "Unlawful Acts Regarding Computers and Information Services".**

Mr. Berghel:
We'll carry this over for the next meeting as well.

**14. Discussion and possible action on request for Nevada Legislature to pass joint resolution calling on Nevada congressional delegation to expand online privacy rights under federal law.**

Mr. Earl:
Nothing additional but my recollection of in terms of how a legislator would move forward with a change to the Nevada Constitution under Item 10 is pretty much the same way that any joint resolution would be handled. If we are moving forward drafting one joint resolution which would have the effect putting forward an amendment to the Constitution, we might view this other as simply yet another joint resolution to be formulated. Is that fair?

Mr. Kandt:
I think what Jim is saying and I would agree is that with both the proposals under Item 10 and 14 – they are pretty straightforward. You've already taken action on Item 10. I think you could take action on Item 14 without any specific language because that would actually be drafted by LCB upon the legislator's request. If you wanted to take action on 14 today, and then those are ready to go to the Tech Crime Advisory Board for their consideration, and then, possibly being picked up by one or more legislators.

Mr. Elste:
Should we develop a draft of what that request should look like so that it's more formalized in terms of what we're asking them to produce without necessarily producing the actual resolution that they are going to use? Is that the next logical step for us?

Mr. Kandt:
I don't think it's a necessary step, that's up to you whether you want to do that or not but just in terms of presenting it to a legislator, I don't think you even need that much specificity.

Mr. Elste:
I would tend to advocate for us providing some specificity so that it was clear what we're asking that legislator or the Tech Crime Advisory Board to agree to and take forward or what we're asking the legislature to do. I think if we put it out there as a request for

them to have a joint resolution calling on Congress to expand all online privacy rights, it begs the question of what we mean by that. I would advocate for us putting some text to describe what we mean by that request.

Mr. Berghel:
Jim, would you be willing to work with Jim Earl on a draft of that kind of language for our next meeting?

Mr. Elste:
I would if Mr. Earl would.

Mr. Berghel:
So be it, we will roll this over to the next meeting.

**15. Discussion and possible action on proposed amendments to NRS 170.045 to authorize the application for and issuance of search warrants by electronic transmission.**

Mr. Berghel:
I believe this is yours, Mr. Kandt.

Mr. Kandt:
It is, Mr. Chairman. This proposal, if you look at Agenda Item 15, I brought to the Tech Crime Advisory Board, itself, at their last meeting in March and they referred the proposal to you for your possible input. The whole genesis of this proposed amendment to NRS 179.045 that I drafted really came about as a result of the U.S. Supreme Court ruling last year in *Missouri v. McNeely* and it had to do with a DUI case and the issue of getting a blood sample from the driver that the officer had probable cause to believe was driving impaired. As a result of that ruling, the issue came up about the ability of law enforcement to apply for and obtain a search warrant in a timely manner. The fact that the search warrant requirement obviously is embodied in the constitution but then the process itself is set forth in this statute.

The statute, in its current form, really doesn't allow for technology because there is technology available now and technology being utilized in other jurisdictions whereby the law enforcement officer via secure line can dial in their probable cause affidavit to a judge and a judge, on an IPad for instance, dials back with a digital signature the issued search warrant with some other subsequent actions taking place but nevertheless, we don't have that authority in our statute to use that type of technology.

I drafted this language and law enforcement is supportive; I took it to the Nevada Sheriffs and Chiefs Association, they are supportive of it; I took it to the Nevada Prosecution Advisory Council, prosecutors are supportive of it; judges that I have shared it with are supportive of it and it's being taken to the Nevada Judge's Association; I shared it with Vanessa Spinoza at the ACLU. She indicated that the ACLU from her standpoint would have no problem with it. I took it to the NAACP at the

request of Senator Ford at the Tech Crime Advisory Board Meeting. They didn't indicate that they had any actual problem with it. Once again, I was asked by the Tech Crime Board to bring it to you for your review and consideration and that's why we're here.

Mr. Berghel:
Would you change "reliable" to "secure and reliable"? Make is clear that confidential data that shouldn't be sent on non-secure media.

Mr. Kandt:
To the extent that there are other statutes that mandate that data transmitted in that means must be encrypted. I think you are referring to NRS Chapter 603A – am I correct?

Mr. Berghel:
That might be it – I don't know for sure.

Mr. Kandt:
So to the extent that there are certain requirements for the transmission of such data under Nevada law those requirements would obviously apply.

Mr. Kandt:
So "secured electronic means" would give you a greater level of comfort?

Mr. ??
I would just leave "secure and reliable". I think reliable is important but secure is a part of it.

Mr. Berghel:
I would add one more thing to that. Secure doesn't mean anything to me. You might mention something like "FIPS 140-2" there are federal standards for such things. I would certainly say referring to a standard like FIPS would seem to get you a little farther along in the civil libertarians trust.

Mr. Elste:
I have a couple of observations to share on this one. First, let me agree with you and Dennis, Hal, because I think we should insist on encrypted communication because you don't want something of this nature being sent out through a clear channel so securing encrypted electronic means should be the standard and we can reference the encryption law that Nevada has on the books which defines to Hal's point, the FIPS standard or other forms of encryption that will be suitable.

My larger concern relates to the use of the term "electronic signature". I'm going to poke a few holes in the existing definition of electronic signature because it does not provide you with a reliable signature mechanism as that is understood from a technical perspective. I can take a digital image of your signature and I use that as a means of

an equivalent to that digital or real world signature. However, that type of mechanism provides absolutely no reliance on electronic exchange. What we need to be able to do is something of this magnitude of importance is apply true digital signature technology to be able to validate beyond any sort of question, that the magistrate or the other two parties in that transaction have actually digitally signed those documents. We cannot rely on 719.100 as effective means of electronic signature.

Hal, I'm sure you understand the mechanics as well as I behind certificate authorities and true digital signatures but in this case, and I'll read to you 719.100 which says, "electronic signatures means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign a record." All fine and good but with electronic construct, I can duplicate your electronic digital signature all day long and you cannot differentiate between my duplication and you intended electronic signature. That's why true digital signatures, certificate based digital signatures, are the standard for electronic signing of documents.

Mr. Berghel:
I agree entirely with what Jim Elste just said. I would add a third element to this and that is I think we need to very clear about retention policies here because there are serious implications when this stuff hits the wire and starts flying around that we need to know who is going to be the holder of these records and how they may be released and used for various purposes. Those three things really need to be dealt with: 1) what does "security" mean; 2) what is a reliable means of authenticating the signature; and 3) what is an adequate records retention policy that guarantees that this information will be recorded and available in legal circumstances?

Mr. Kandt:
With regard to the third one, everything that applies for the existing process for applying for and issuing search warrants and how that data is retained would apply. With regard to the first and the second, the security of the electronic transmission and the authentication – can you help me with that – I am trying to get this passed so that law enforcement can utilize technology and ask for your help in how we can revise this to give you the comfort level that you have and hopefully, get it submitted.

Mr. Earl:
One observation and one suggestion: the particular statutory provision that Jim Elste just read, NRS 719.110, was actually passed probably around 15 years ago. It carries the title "Electronic Transaction Uniform Act". It almost undoubtedly, although I wasn't around Nevada at the time, was passed by the Legislature as just one more, additional uniform act that was appropriate for passage. I can recall some of the early work being done at least 20 years ago.

Based on what Jim Elste just said, joined by the Chair, it's pretty clear that the definition of electronic signature would achieve general acceptance through the uniform act process of which is pretty extensive, it takes years of hearings before the American Bar Association and other entities for something to be identified as a uniform act. Whatever

process and however rigorous it may have been 20 years ago, has been overtaken by technological advances. It would be open for us, looking at the draft text we have here, essentially, to strike the reference to the existing Statute 719.100 which, in the normal course is what you would try and do. Try to refer to another portion of Nevada Statute in order to incorporate an appropriate definition.

Here, the passage of time has rendered this definition inappropriate. It is open to someone making a legislative proposal to create a new definition of this term and to lay it out in the statute. You could say, as used in this subsection, electronic signature has the following meaning ascribed to it and then define the term as you felt was appropriate. That's my first observation.

The other observation and I say this now having more interest in it than I would have a year ago, the organization to which I am presently a member, Enterprise IT Services, has picked up all of the IT functions that were previously performed by the Department of Public Safety. If, in fact, were the Legislature were to move forward on legislation like this, I can represent to you that it would come at a cost because, at present at least, there is only minimal encryption capability available to first responders. That may change over a period of time and the first proposal which will be implemented sometime five or 10 years out is designed to attempt to address those issues. In order to provide meaningful encryption from first responders, less specifically law enforcement officers, not just state law enforcement officers, there would have to be an investment in new technology for this to occur from most locations that are remote or mobile.

Mr. Kandt:
This is just enabling legislation, not a mandate, and to the extent that agencies don't have the funding or resources to implement an "e-warrant system" as some vendors market it, then those agencies will continue to use their traditional means of applying for and obtaining search warrants. Once again, this is enabling legislation. Right now, even if they had the funding and resources available to utilize an e-warrant system, they don't have the statutory authority to do so. That's why I would really like, since our Legislature only meets every two years, to get that authority put into statute during the 2015 session.

Mr. Elste:
I think it's an excellent piece of language; the intent behind it is really good and I certainly and whole-heartedly support advancing law enforcement into the digital age. I think, with a few adjustments to some of the things like digital signature, two things happen: you get a really good piece of language for enhancing or adding that e-warrant language to NRS and the other is, we are actually going to produce the ability for law enforcement to start implementing technology that lets them have things like digital signatures and secure communications through means like tablets and so, it's the greater good in my mind, to make something like this happen. It's just making sure the language is solid enough so it doesn't go out there and they do it in a way that is somehow substandard from a technology perspective. I'll commit to helping you refine the language.

Mr. Lichtenstein:
This isn't really a part of this issue as he said, he's spoken with Vanessa and we have no problem with this particular language or concept but I think it's fair warning is that I plan to testify whenever this particular thing comes up and ask for language to be put in there that guarantees no search warrant will be executed until it is actually signed and returned because I have seen in the last year, too many that were signed afterwards and that's not an electronic kind of issue but just to know that while we would support this kind of language and this kind of process, even current rules are not always followed.

Mr. Kandt:
Just to clarify, when you say signed and returned, you mean as envisioned here, signed and returned in a manner authorized electronically.

Mr. Lichtenstein:
What I mean is, basically, I've seen search warrants executed when the judge signed it afterward the fact. That was not that uncommon to make me think that this isn't an actual practice.

Mr. Berghel:
Would you have a problem, Allen, if the signature of the judge was applied electronically by them putting their fingertip on a reader?

Mr. Lichtenstein:
I have no problem with that. Hopefully, doing something like this will avoid or help avoid some of those kinds of problems, I'll be asking for language that says "signed prior to any search warrant being carried out."

Mr. Berghel:
Something else before we move on to the next item, I might to accept that the electronic information management of this is covered by other statutes, but once this gets into the digital realm, there's virtually no end of morphing that can take place. It has to do with time stamps, signatures, all of this has to be spelled out in the statute to guarantee that whatever did happen, happened exactly as it is represented. That needs to be anticipated in the statute. With that said, I urge you to keep working with Jim and others and bring it before the Subcommittee next time.

**16. Discussion and possible action on possible revisions to the statutory definition of "personal information" in NRS 603!.040.**

Mr. Kandt.
I believe Agenda Item 16 was actually suggested by Dennis at the last Tech Crime Advisory Board meeting whether the definition of personal information in NRS 603(a).040 needs to be reviewed by this Subcommittee and possibly recommendations made for updating or revising it.

Mr. Cobb:
Nothing to add.

Mr. Berghel:
Let me suggest that we roll this over. There are FIPS standards for PII and I suggest that we look at them. Let me give you a reference both you, and Brett and Dennis, there's a special publication that NIST has produced called Special Publication 800-122 and it defines PII. It includes a fairly encompassing definition that I, personally, am partial to so I think it's worthy of our attention.

Mr. Earl:
I'd like to complicate this a little bit. I'm familiar with that PII definition and I agree with you. I like it. The one issue that I think is problematic is that about two years ago, at the time it was likely that the U.S. Senate was going to take action on an omnibus cyber security bill, there were multiple bills in both the U.S. Senate and House to redefine both the PII definition and to insure that the federal definition and its application pre-empted the state laws definitions of PII. There were a multiplicity of different definitions of PII that were contained in these various bills. To the best of my recollection, there were at least a couple of bills that defined two different types of PII.

The position that I had at the time, was that it wasn't necessarily a bad thing if the federal government wanted to pre-empt the various state definitions of PII but what would have been important and I was not in a position to speak for any state attorney general at the time, was that at least some of the legislation would have operated in a way so that the federal government was responsible for certain types of enforcement in PII breaches. The state attorneys general were responsible for others. The problem was that way in which some of the federal legislation was crafted is that it would increase the responsibility of state attorneys general so that they became responsible not only for enforcing the existing state definition of PII but took on the additional responsibility of enforcing the new federal definition which did not coincide with the traditional state definitions of PII. I was concerned that any federal legislation, even if it pre-empted the field, did not make sense if it placed additional burdens of enforcement on state attorneys general.

None of that legislation actually passed and I'm not aware because I haven't have reason to look or do searches for federal legislation, I simply don't know whether there is any comparable legislation that is now pending. Some of the proposed federal statute definitions of PII came close to the NIST definition that you just cited and some were at variance with it in some important ways. I just want to alert everyone that in the past, there have been a couple of moves at the federal level, none of which has been successful, to redefine PII in a way different from the existing NIST definition and in my personal view, at a way which would complicate the workings of states attorneys general in trying to enforce data breaches that involve PII.

DRAFT

Mr. Elste:
I'm afraid I have a slightly simpler comment than Jim's observation on the federal and state implications of PII which is that the term "personal information" is actually a little out of step with common nomenclature and we should consider changing it to "personally identifiable information" because that is, in fact, what we are talking about. As you've heard references to PII, we should update this so that if reflects what is now a common term of art which is now "PII" or personally identifiable information in referring to an individual's name and identifying information like driver's license number, etc., so if we do take this on, let's try to update the title.

Mr. Earl:
When I made my comment, I didn't mean to indicate that this as a criticism of the NIST standard. As a matter of fact, we might be doing both ourselves and other states and citizens throughout the country a service by being one of the first to adopt the NIST definition. If a state or series of states adopted the NIST definition, it would become increasingly unlikely that legislation at the federal level would veer off very much from this definition. As a matter of fact, the state definitions of PII are essentially are all traceable back to a state law that was initially passed in California.

Mr. Berghel:
Just FYI, Jim Elste, this does use the term "PII", it's already stirring with the world. It's ours that needs to be updated.

**17. Committee comments. (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.**

Mr. Berghel:
Any Committee comments?

Hearing none, next item.

**18. Discussion and possible action on time and location of next meeting.**

Mr. Berghel:
How do you feel about meetings over the summer?

Mr. Kandt:
I just want to emphasize the time constraints you are facing with any proposed legislation. Obviously, any proposed recommendations of this Subcommittee will have to go to the Board at one of their regularly noticed meetings. That process will have to take far enough in advance of the deadlines that executive branch agencies and .legislators face in proposing legislation. For instance, the Executive Branch, we have to have our bill draft requests into the Legislature by the end of August. So that's a pretty narrow time frame. Legislators have a little more flexibility but nevertheless, as you come up with legislative proposals to allow sufficient time to figure out an avenue

for getting that proposal introduced into the Legislature. Time is very much going to be a consideration.

Mr. Berghel:
Point well taken.

Mr. Earl:
I absolutely concur with Brett.

Mr. Elste:
I'm wondering if we can sort of back into an agenda for this group based on Board meeting schedules and the need to submit requests for legislation through that body.? That would also align with us having items for action on those agendas so that we could adopt language or proposed bill language that would go to the Board. Can we back into that schedule?

Mr. Kandt:
Yes, a couple of things I was going to recommend that anything from here on out that we are carrying over be listed as an action item. The next tentative date, we were looking at a meeting in early June would be the next quarter on a quarterly meeting of the Board. The first week in June, provided the Board wants to meet then, would you want to hold one more meeting before that Board meeting to try to have some proposals approved that the Board could then consider if there is a meeting in June.

Mr. Berghel:
Yes, I think so. I guess we'll have to do this the way we did before. Are there meeting times in late May that are a problem for anyone on the Subcommittee? Members are to check their calendars and advise Mr. Kandt of their availability for the last two weeks in May tomorrow.

**19. Discussion and possible action on future agenda items.**

No further comments.

Mr. Berghel:
Do I hear a motion for adjournment?
Mr. Lichtenstein moves to adjourn. Mr. Elste seconds the motion. Meeting adjourned.

DRAFT