TECHNOLOGICAL CRIME ADVISORY BOARD
Technical Privacy Subcommittee

MINUTES OF THE MEETING

February 21, 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; James Earl; James Elste; Ira Victor; Dennis Cobb.

   Absent: Allen Lichtenstein.

   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 second meeting and stated he was encouraged by the work that has been done in the last two months.

4. Report from Hal Berghel on comparison of Nev. Const. Art. 1, Sec. 1, and Cal. Const. Art. 1, Sec. 1, "Declaration of Rights."

   The reason that I added this to the agenda, I don't really know what to do with the fact that we don't have privacy explicitly mentioned. This is a question that I address to the lawyers that we have. Is there a clear and obvious way of including privacy in the constitutional framework in Nevada without actually going through a constitutional amendment?

Brett:
Obviously, there's case law in which courts have construed a right of privacy within the constitution and to the extent, it's delineated through case law. In terms of an explicit right, that would require an amendment.

Hal:
What is the downside of not having privacy explicitly articulated in the constitution?

Brett:
Whether it is explicitly delineated like it is in the California Constitution, or it is implied through case law, you are still going to have it subject to interpretation by the courts as to what the extent of that privacy is.

5. Report from Allen Lichtenstein on possible language for a proposed amendment to the Nevada Constitution establishing a right to privacy.

Hal:
Since Allen is not here, let's hold off on this item.

6. Report from Allen Lichtenstein on project to identify all Nevada Revised Statutes that affect privacy rights.

Hal:
We will get back to those since this is Allen's as well.

7. Report from James Elste on request for assistance from Electronic Frontier Foundation to develop legislation to expand online privacy rights.

Jim Elste:
I regret to report that I have not acted expeditiously on that request. I did have that discussion with Jay Stanley who expressed an interest in the work that we are doing. He is the Senior Policy Advisor for the ACLU in Washington, DC and he would be more than willing to support the work we are doing and come and provide presentation or otherwise interact with our subcommittee. I have not reached out to Lee Tien, the senior staff attorney at EFF but I will do so and report back to the board at our next meeting.

Hal Burghel asked Brett Kandt if this agenda item can be carried over to the next meeting and Brett replied certainly.

Hal asked Stephen if he had connections with the feds as well. Stephen stated that in years past, I knew Mike Godwin. I don't know if he is still affiliated with them or not.

Hal:

Certainly, the more avenues we pursue, the better. I see no reason not to.

Stephen:
I will get in touch with him.

Hal:
I would like this carry-over item to include that Stephen Bates will reach out to Mr. Godwin.

Ira:
Lee Tien seems to be keeping an eye on what's going on in Nevada and I have spoken with him on previous legislation so I think he would be a good person to reach since he is aware of some of the legislation that has happened here in Nevada.

Jim Elste:
Lee was very helpful when it came to the BDR we had in the last session and willingly put us in contact with the EFF attorney that was working on the litigation on the mega-uploads case. He has already demonstrated his willingness to help out in Nevada and a willingness to help out efforts that involve developing new statutes. I would fully expect that he would continue in that capacity and willing to help us out.

To be blunt, I just did not have the opportunity to reach out to him and start a dialogue on this.

Hal:
Would he be willing to join us at our next meeting?

Jim Elste:
I would be happy to ask. Lee is out in San Francisco so it's not, by comparison to Jay in Washington, DC, it's a little more feasible geographically for Lee to participate. I will reach out to him and get a dialogue started once we figure out the next meeting date. I will be able to give him some specifics and I will be happy to invite him if that's the will of the board.

Brett:
I just wanted to mention that Dennis Cobb has joined us on the phone.

Hal:
Can you ask him if he is ready to speak to us on his notional information security taxonomy.

8. Report from Dennis Cobb on possible revisions to the State of Nevada Online Privacy Policy.
Dennis:

I don't know if the document that Brett sent out made sense for everyone but it's the basic premise is to try to describe the framework for information in the State of Nevada so that there is not a blanket requirement for security.

Brett:
If I understood you correctly, Dennis, you just wanted people to ask questions of you based upon the written material that you submitted to the subcommittee.

Dennis:
Yes, it's a notional thing, it's not meant to be prescriptive that it has to be that way. The basic objective is to try to get the framework that allows just a few different categories of information so that when it is shared between agencies in Nevada, the distributing end can say "are you equipped to handles Level 1 or Tier 1" or whatever we want to use for a name. That kind of information – the receiving end can say "yes, I agree to handle it to that level of security" so there's an agreement ahead of time on how it will be cared for.

It isn't meant to replace any existing classifications at all, HIPAA and all the other requirements that have come out will have to deal with it. It's just meant to allow people or organizations to exchange information with some previous agreement of understanding on how it will be handled.

Jim Elste:
In some respects, this is a security standard for a classification scheme that would be used regardless of the type of information privacy related, confidential state information, as the way it is outlined, around the potential for loss, for disruption, harm to people and organizations, etc. I have a question about whether or not we are treading into the domain of the State's Chief Information Security Officer and Office of Information Security in putting this forward as opposed to trying to collaborate with them and otherwise see what they have and what they doing. My sense that privacy defines the what it is we are protecting based on the type of information it is. Personal information, health-related information, things of that type. The job of the security officer is to define the how we protect it so where this taxonomy has some rather high level but prescriptive guidance as to what needs to be done from an encryption perspective. I fear that that might be the domain of the Office of Information Security and the State's Chief Information Security Officer.

Dennis:
I can see your point on that and I think that may be true. The way I see this is that it's to facilitate agreements so that you have essentially a contract between a sender and receiver of information on how it would be handled. It sort of set parallel or apart from statutory and regulatory requirements. I can see this being more of a Best Practices way of doing things and not so much that it's written in as a must do. It's a model for reaching agreement between two parties that have information they need to share.

Hal:
It's an excellent model. I think the thing we might do is use this as a form of outreach to the Office of Information Security and see if they have something and if they don't, here's a suggestion that could start a dialogue and help them foster that type of taxonomy.

Jim Elste:
It's just my experience that the federal government uses four tiers, with official use only, that classified, secret and top secret are the three broad categories they use is that all off those have implicit requirements on senders and receivers of what their duties and responsibilities are of the information. I didn't want to go in that direction with those terms but I just used that model of three-tiered framework. Would you object if I took this as an action item and recap this to Chris Ipsen and discuss this and report back next meeting?

Hal:
Would either of you object if I took this as an action item and recap this for Chris, discuss, and report back next meeting?

Brett:
Just to clarify, you want it listed as an action item for the next meeting?

Hal:
I will report on the response from Chris Ipsen, the Chief Information Security Officer for the State of Nevada.

9. Report from Stephen Bates and Allen Lichtenstein on possible changes we might make to the news shield law.

Stephen:
Nevada has one of the better news shield laws in the country in terms of insulating journalists on having to testify in various proceedings about both confidential information and other information they have gathered in reporting. It is rather dated in terms of who is encompassed by it, in particular, news media organizations. It is also a bit off in referring to former employees of certain organizations but not of others. You have to be a current employee of some types of organizations. These issues have arisen in other states – authors and scholars who have tried to claim the privilege as well as free-lance journalists so the first of the three things was an attempt to encompass a broader population under the shield.

The second is a rather specific issue. Some of you may know Dana Gentry, a journalist based in Las Vegas who works for Jon Ralston, was subpoenaed and the effort to get around the news shield law was "we're not trying to get anything related to reporting, we just want to look through your personal, private financial

records to prove you were taking bribes. The bribes fuel your reporting." The Nevada Supreme Court rejected that and said that still is about reporting. Nonetheless, Allen suggested a phrase or clause to bring that more explicitly into this news shield law.

The third thing which was suggested I to report to this subcommittee is third party subpoenas and that language was largely taken from the California News Shield Law. It is part five concerning giving the journalists notice, in most circumstances, before seeking records of a telephone company.

I put that together and if you take a look at it, would welcome thoughts.

Hal:
Any questions or comments?

Jim Elste:
I love the fact that we are now defining what a news organization is and the question I have is whether or not non-news journalists would be protected with the language you have defined. For instance, an author who is researching a book or other form of researcher who may be gathering information just as valuable as a news journalist and entitled to the same sort of protection. Is there a way to make sure this is encompassing for non-news journalists?

Stephen:
It mentions book publishers which I hope would encompass people who actually have a book contract. For free-lancers, the Vanessa Leggett case from Texas a few years ago, there's no easy way to cover her. She was a free-lancer who essentially had no clips and no book contract but was seriously working on a book project. It's hard to find a way of defining her that wouldn't also bring in almost anybody. One does want to have a distinction between a Facebook status update and slight magazine. I think we use language on a regular basis to disseminate information on current events.

Jim Earl:
Question: In putting this together, were you in contact with anybody from the Nevada Press Association? I may not have the name correct but I know that there is such a group and their headquarters is within a city block of here. I raise that because I don't know whether their executive director has remained in place for the last 6 years but if it is the same one who was through a couple of the previous legislative sessions, I know that they have a relatively continuous presence during legislative session.

Stephen:

I mentioned the general issue to a couple of people who are associated with it but I haven't formally run this past anyone.

Jim Earl:
I raise this for a couple of reasons – one, purely a political one, if there were a decision either by the Attorney General or by anyone else, a legislator for example on the Tech Crime Advisory Board, to move forward with sponsorship of something like this, we would clearly want to ensure that it was at least consistent with whatever the Nevada Press Association was thinking. The second reason is it would seem highly likely to me that they have coordinated language among other state press associations on the issues of how best to consider expanding existing news shield laws. They would be a valuable source of input for anything that we are considering as well.

Brett:
I have worked closely with Barry Smith who is the Executive Director of the Nevada Press Association on a number of issues regarding transparency in government and I'd be happy if this subcommittee is comfortable with me sharing this proposal with Mr. Smith in getting his feedback.

Stephen:
I'm fine with that in terms of the first thing – absolutely, they would have to be involved in any such effort. I'm sure they would have valuable input. As far as the second, to see how other states have done it, I don't know that there is a very good model yet. I asked the reporter's committee and they didn't have a lot of guidance. A professor in Indiana has put together a monograph looking at how different states define a journalist based on employment versus a functional approach. I don't know that there is a best practice. I would welcome the input of the Nevada Press Association.

Hal:
Can I ask Brett to send the contact information to Stephen and Allen and you are welcome to get engaged on your own but I'd like the authors to be directly communicating with the Nevada Press Association. I just think it's a better way to do it to have the people who are writing the draft to be able to make the modifications directly rather than triangulate.

Brett:
I will facilitate bringing them together.

Hal:
I would like to interject something because I was affected by this just a few months ago. I think this is commendable that we are trying to do something but my experience is that the possible intimidation that can result from the fear of prosecution is extremely broad. In the case that I was involved in, the threat wasn't directly relating to the shield, the threat was on the business model of the

corporation that was publishing the periodical. If a professional publisher loses all of their circulation, or a not for profit professional organization loses all their members, you have the same effect as censorship. It's just a corporate approach. I think that we are doing something that could possibly be of great benefit. I encourage of all you if you have any ideas, send them to Allen and Stephen and see if we can make this as encompassing as possible for all of our sakes.

10. Report on possible changes to NRS 205.473-.513

Hal:
What I have before you is a straw man and I want to preface my suggestions for NRS Chapter 205 as admittedly sub-optimal approach to this. This is my first attempt at drafting statutes and I might add, I am singularly unqualified professionally to do this. It occurred to me that NRS Chapter 205 was fundamentally flawed and if it weren't for the fact that I don't really know how to fix these things, my recommendation to the committee would be just to erase it and start all over again. However, the problem is there is a fabric to these interrelationships and you can't go pell mell into the statutes and expect everything else to stay unbroken. With that in mind, I am reaching out to the attorneys on our subcommittee. I would like someone, an attorney, to help me draft this if the subcommittee thinks that there is some possible advantage to it. It takes a long time to do this, many hours were spent on this and so if we, as a group, think this is not profitable, I'll be happy to drop it. I would like to see us go forward but I would have to do it with an attorney.

Jim:
Point of clarification – are you willing to accept help from non-attorneys that have experience with drafting statutory language?

Hal:
Certainly. The bottom line is that at some point, we ought to have an attorney involved in this. I will take that as a volunteer for your time.

I don't want to go into any great detail here but if you would carefully look over this proposed revision and if you have any thoughts about this, kindly send me an email and I will work with Jim Elste and whichever of the attorneys on our subcommittee volunteers to take this to the next meeting.

Jim Earl:
I am actually looking at the very carefully and professionally drafted test which you have provided.

Brett:

I think Jim is thinking as I am of the fact that you will all work so hard and come up with something that is perfect and then we go through the process of submitting it to the Legislative Counsel Bureau and perhaps the biggest battle is ensuring that the language that you carefully crafted and the substantive component to that language doesn't get corrupted in the process of the Legislative Counsel Bureau drafting it into a bill. That, in my experience, is the most difficult part. We will cross that bridge when we come to it.

Jim Earl:
The other thing that I need to mention and why I have not raised my hand as a volunteer before this is I'm also involved in essentially redrafting and rewriting the basic statute that goes to the provision of state information technology services. That is a single chapter within the Nevada Revised Statutes but it has hooks into at least as I write it, about three or four other major statutes. I have my own very major statutory drafting exercise under way. I will be glad to help with this but need to provide the caveat that I've got a major statutory rewrite in my day job.

The other observation that I think does bear mentioning is that as you probably have noticed by working with the statute just on a line in line out basis as you have, it appears to me that the last major modification to NRS Chapter 205 appears to been made – one was made in 2011 because I introduced some language to protect state workers who were running penetration tests but prior to that I think the last significant modification probably was in 1999. That was prior to the time that the Tech Crime Advisory Board came into existence. Bottom line, this statute hasn't been seriously looked at in quite a long time. And, an even longer time in the IT world and web chronologies so it's certainly due for a major rewrite/relook. I think that it is possible to justify to the legislature a basic re-examination even on that basis. Given the amount of time that I spent in legislative committees in the last legislative session, the degree of concern that I found expressed by legislators about information technology issues generally and IT security issues more specifically has been increased probably several fold over the past five or six years. In no small part due to the actions of the Tech Crime Advisory Board and others. Bottom line here is I think that more so than in the last couple of legislative sessions, the time is probably right to at least request a hard look at a fundamental rewrite of NRS Chapter 205. With regards to my participation, I would be glad to help to the extent that I can. The probability of being able to engage either the Attorney General or one of the legislators on the Tech Crime Advisory Board in such a fundamental relook is probably higher now and higher in the next legislative session than it has been in the preceding two or three. That's not to say that this is going to catch fire but the amount of interest in the general public about IT and IT security has certainly been effectively raised and that would bode well for a fundamental relook.

Brett:
Jim, what is the chapter you are rewriting just for reference?

Jim Earl:
NRS Chapter 242.

Ira:
There is one element that I would like to bring up that permeates a lot of the great work you did. Speaking as a non-attorney, and that is when you talk about consent. I think that one of the issues as I've looked into this in the past, is the notion of informed consent. For example, we have the well-known case of an app for smart phones and tablets that turn your camera flash into a flash light. It was actually tracking your location and selling information to advertisers. People consented to the flashlight but did not give the informed consent about the tracking and the other issues. I think throughout it, the notion and I don't know if the best way to say it besides the plain language of "informed consent" would be a good addition.

Brett:
With regard to apps. in general?

Ira:
There's a lot about consent in here but adding the words informed consent, adds an element. Everyone clicks on an end use license agreement – that's not informed consent, I would argue. Not always informed consent when you click on an end use license agreement and ULAs.

Hal:
Could I encourage you to send me a very brief email on your thoughts and we will make sure that your points are addressed in the next draft. Jim Elste, admittedly you are pretty small on the screen but you look like you have a comment.

Jim Elste:
I did have just a brief observation which is when we worked on the amendment to NRS Chapter 603A and attempted to revise the language around encryption probably one of the most important lessons I took away from that was to try and craft the language in a way that doesn't include such high degrees of specificity that it becomes obsolete very quickly. Technology changes very rapidly and as Jim rightly observes, a statute that appears to have been originated in 1983 bears very little resemblance to the technology available in 2014. The degree to which we look at the problems with NRS Chapter 205, I think we ought to keep in mind that language that has the ability to define what we are trying to address without incorporating extremely specific references to technology or specific exploits in the case of malware because those things can suddenly become obsolete in the language and otherwise undermine what is a well-intentioned effort to encapsulate a very strong concept like protecting a computer from malware, things like informed consent. I think a review of NRS Chapter 205 is well overdue and I look forward to working with you trying to do this because this

is fertile ground for some really sharp security guys and some attorneys to get together and come up with some good language.

Hal:
Since you brought this up, I would like to comment on your observation because it's a very poignant one and that is when I started to re-write this, I used what appeared to me as a novice, could be the same sort of granularity that was in the original statute. If I saw the specifications were made as to certain types of secondary storage and they had forgotten some of the modern semiconductor storage, I'd just add the semiconductor storage. I did that because I was afraid that if I went too general, it would undercut the effectiveness of the statute. That said, I think your suggestion is a much better way to go if the statutes will tolerate it and that is you just say digital storage and don't specify the ratings of the system, we don't specific the mechanism. It's just digital storage. Jim Earl, what happens if you take all of that wording out and just use terms like digital storage.

Jim Earl:
It depends on what the major concern there is that the terms you will have eliminated may be picked up and used in other portions, either this statute or of some associated statute. That's a real difficulty when you are dealing with an entire statutory regime that has become, in some sense, decompartmentalized. The present version of Nevada Statutes that we are dealing with are codified as the Nevada Revised Statutes. That is an indication that there was a major revision and Brett will know when that revision was and I don't, but sometime within the last twenty or thirty years there was a revision of the statutory scheme that existed prior to that. That was an attempt to consolidate statutory provisions that had grown sort of haphazardly into a consolidated scheme. Now that the Nevada Revised Statutes have been in existence for probably three decades, we essentially see the same thing happening all over again. Bits and pieces of statutory text are added or referenced here so what began as an overall, fairly well organized statutory plan has become less organized because of the way in which individual legislators have adopted amendments. Part of the problem in statutory drafting is trying to ensure that the section you are dealing with is changed only in a way in which that do you understand the ramifications.

Hal:
You are talking about don't change anything that is going to break a lot of other things.

Jim Earl:
What I'm talking about is the need to be cognizant that that is a potential risk. The good news is that the IT statutes have been relative to some other statutory schemes, fairly well isolated. In other words, there's not as much cross referencing as there can be in some other statutory schemes. That is always a potential problem and it is something to be cognizant of and to its credit, the legal staff at the Legislative Counsel Bureau tries to highlight terms that are used in

different statutory locations. They are aware of this general problem and they try, in the statutory text, to highlight terms that are cross referenced. That is a potential danger whenever one tries to rewrite statutes. That is common and we need to take that into account. It is certainly not a reason not to go forward, it's simply a reason to recognize that changes can have effects on other statutory schemes potentially.

Jim Earl:
The other thing that I found to be very helpful is to use or reuse statutory terms rather than try to redefine them. For example, I noticed in there that you used the term 'steganography' which has not been used before I don't think in other statutes but also used the term 'encryption' and what I would encourage and try to help us do is rather than redefining encryption in NRS Chapter 205 to use the statutory definition that exists in NRS Chapter 603A, if we possibly can. This is just an example.

The other thing that I wanted to add is that Jim Elste and I have spent a fair amount of time a couple of years ago coming up with a very, very short statutory fix at the federal level of what we thought would eliminate the need for or greatly reduce the need for the complications that successive federal legislators have tried to add to the federal regime in 200 page-plus omnibus cyber security bills. We produced what we thought was a pretty tight and very workable and pretty short definition of malware so we didn't have to redefine viruses as distinguished from worms as distinguished from something else. One of the things when Jim and I looked at this, we tried to take the lessons that we learned in that drafting exercise and apply them here. That would affect only a fairly small portion of the way in which you've set this up and to your credit, the definition sections that I read are consistent with what we've put in other definition schemes. We just try to bind them together a little more tightly, if that makes sense.

Jim Elste:
Another observation – I'll refer the way we refer to the language was to add 88 words and subtract two and accomplish what they tried to accomplish with 100 or 200 page omnibus bills.

The other thing and I think we may have an opportunity to further the technologists in the house and add some value. We could, literally, have a big data exercise on NRS and take all of the NRS, place that into a database and give us the ability to find and correlate terminology across statutes so that if the word 'encryption" appears in multiple places, we would be able to identify simply by searching for that term to identify which statutes were impacted by that. It doesn't solve the requirement we have someone with legal expertise look at the language and the context of the language and the intent of the language but it could help unravel the mystery of where are the terms being used or defined or otherwise implicated. From a technology perspective, a straightforward exercise is to basically subsume the NRS as a digital document into a database, give you

the facility for using database searching predictive analytics to determine where particular types of language are going to have impact. I think things like that would give us a facility that takes some of the challenge associated with this out of the manual arena and put it into the automated arena because even the best attorney in the world is going to be daunted by the task of going through NRS, finding every reference to a term like 'encryption" and figuring out where they are. To me, a bit of a Gordian knot of statutory language that isn't necessarily, it doesn't have an index, it doesn't have the types of things that help you understand where that language appears.

Jim Earl:
One of the things that I have so far, unsuccessfully, tried to do is get people in my division, and the State, interested in non-relational databases. So far, I have succeeded in failing miserably. It is exactly the type of exercise that Jim just described that might be pitched not simply as an aid to the legislative process but as an exercise that would demonstrate the difference advantages and disadvantages between relational and non-relational databases. I approach this as a definitely lay data base user and is certainly not a database designed is that if properly put together, the type of search that Jim described will be a whole lot easier in a large non-relational database. I defer to those of you that actually know what you are doing.

Brett:
To clarify for the discussion, the NRS has a searchable database but it is a non-relational database, correct? You can enter the term 'encryption' and you might get some useful hits because it's a fairly unique term but if you used a term such as 'data' you are going to get garbage. That's where the benefit of a relational database. I don't know if anyone has had that conversation with LCB or not. I don't know if LCB has a separate database for their own exclusive use that they use that has more of a relational search engine in it or not.

Hal:
If there is any technology that we could use that's available to you folks, I'm all for it. Let's go for it. I have a question though, this is question from a neophyte, having built a couple of digital libraries in the 1980's, we went through this problem at a very superficial level, in the publishing business because we get a couple of trillion pages of information, we wanted to know how they were inter-linked by concept and so the publishing community paid for and developed in the 1970's, SGML. You may not be familiar with SGML but there was a hobbled descendant of SGML called HTML which was used to create the worldwide web. The point that I am trying to make is that this concept of hyperlinking dates back at least till the late 1970's. Why is it that the statutes aren't hyperlinked in such a fashion? Is there a reason for that?

Jim Earl:

I think they are, I'm not sure that it's terribly well done but if you go to the online version of the NRS on the legislative website, there are a number of hyperlinks that do, when activated, bring you to another statutory provision.

Brett:
Just to follow up, in addition, you'll also note that for instance, going through your draft here for some of these provisions, it will indicate when they were added to the NRS and/or otherwise modified. After a certain date, there is a hyperlink to the Statutes of Nevada that enacted those modifications. The earlier, they have not put in that format. I don't know what the date is – sometime in the 90's, 97 or so, where they became hyperlinked.

Jim Earl:
Essential summary – the folks at LCB IT have done a better job than their counterparts in many other states because, having looked at the statutes in other states, their web presentation, LCB has placed us in a position where we are better than a good number. We are not where we could be, perhaps, given complete exploitation of available technologies but we are better off than where we were. I have used the search mechanism that Brett has described and sometimes it is helpful and sometimes it's just not helpful at all. I think Jim's initial suggestion which put us on the track where we are now was to try and focus on those portions of the Nevada statutes that had either an IT or a security or a privacy link and try to do a more complete indexing of those particular provisions. Quite apart from the general exercise that LCB has implemented with varying degrees of success over the past 10 years.

That was your suggestion, if we could come up with somebody who would be willing to use that as the subject matter for a technology test pad whether that was relating to an IT technology senior thesis substitute or whatever, that would be great. Is that what you meant?

Jim Elste:
That is correct.

Hal:
Let's continue this for next week as a discussion item. We'll bring this up again at that time. In the meantime, Jim and Jim, I will look into the business of how we can best use the facilities available for modifying statutes.

11. Report from Jim Elste and Ira Victor on proposed strategic framework.

Hal:
Jim, there's a lot of material that you have here so I would encourage you to take some time and try to explain to us how we can best use all this material you provided.
Jim Elste:

Today, what I was hoping to convey is essentially a rationale behind a framework for evaluating opportunities to develop privacy legislation. The notion of a strategy assumes that in some form or fashion, you've done an evaluation and determined where opportunities lie and then develop a subsequent strategy as a result of that evaluation. Just to make sure this is on the record, Ira and I met last month to have a discussion about the pieces of this evaluation framework fit together and how they can be applied to the work of this subcommittee. What I did is I put together an overview deck to use as a framing discussion and then an actual evaluation framework in the spreadsheet. Brett did an excellent job of copying the material with one slight exception, there are three other tabs in my spreadsheet that didn't make it into the hard copy. The key points that we need to discuss are readily available in the printed material.

1st Slide, when we met with the Tech Crime Advisory Board last summer, I used Lawrence Lessig's Code 2.0 references to the four forces that shape the world we live in from a technology perspective. It's important to recognize that we have technology that evolves very quickly. We have market forces which adapt very quickly to that evolving technology and then, more slowly what we have is a shift in social norms. Ultimately, laws, regulations and policies are defined to codify or otherwise adapt to those shifting elements. What we have to be able to do in evaluating privacy in particular is look at those other forces, the technology, the market forces and the social norms and evaluate them against the legal practices, the regulatory practices and policies that are going to either enforce advantageous privacy policies or otherwise offset derogatory or negative market and technology forces. We want to be able to synthesize that into something that makes sense and is rational from a policy perspective. It all sounds easy but it's not, of course.

The basis of the framework that we put together was two parts – one took a look at the work of Daniel Solove in his seminal paper on the taxonomy of privacy which defines a series of privacy harms. The harms are in particular descriptions of acts that cause a harm to individual, so as an example, surveillance has an element of harm to an individual's privacy or civil liberty. The way he structures his taxonomy has four parts: information collection process, the processing of information, the dissemination of information, and then what are some rather explicit invasions of privacy. Those 16 privacy harms give us a frame of reference for considering acts or practices that cause the harm to the individual and what we might do to offset that harm or otherwise prevent that harm from occurring. The use of that is really a basis of establishing the consequence of a practice and using that in part as a reference point for evaluating what might be done from a policy or legal prospective.

The next piece is looking at what are desired behaviors or practices and those are found in the consumer privacy bill of rights and the fair information practice principles. I have a slide that highlights the particular elements of that and what you will see is that CPBR and FIPS have very similar descriptions of things like

transparency, individual control, security, but they each have a rather interesting sort of nuance to them when you read the documents. They are not mirror images of each other. They are very good about defining the types of advantageous practices we should be striving for. We should, as Ira mentioned earlier, have informed consent, have transparency as an aspirational practice when it comes to information systems or the collection of information of an individual. That CPBR and FIPS give us a frame of reference for positive practices that you want to see incorporated or otherwise reinforced in statute.

Lastly, the question becomes where to start slicing and dicing this. What I did, was basically look at a hierarchy of where you would compensate for otherwise incorporate either the principles of CPBR/FIPS or the offsets for the harms defined in Solove's taxonomy.

At the bottom of any sort of construct, we have contractual obligations. In an ideal world, contracts would be fairly written and would incorporate the protections that should be there and offset the harms. That is not always the case. We go higher up the scale – we look at the regulatory environment. Obligations that aren't necessarily statutory in nature but are defined by a regulatory regime and enforced on a group that is regulated. Things like HIPAA, things like PCI.

Then we get into the actual statutory language. The Nevada Statutes, we look above that at federal law and ultimately, we can look to international law. That construct gives us a way of not only looking at what exists and how it's layered but it also lets us have a reference point for the types of statutes or language we would want to pursue or otherwise try to define and put into statute in Nevada. At the end of the day, we have to remember we are not writing law for the international community or the federal community, we are doing it for Nevada.

The last slide is really an exercise in how we would apply this framework which is to do a gap analysis. There are some limits in the way I put this slide together. Red is bad; green is good; yellow being in the middle. It's easy to see, represented here, a hierarchy of the law and where we have good law in place that we feel covers a particular element of either protecting from a privacy harm or otherwise encouraging a beneficial privacy practice that is something that does not require additional statutory language. However, where we have instances where there is no statutory language, where there is a harm, or there is an absence of those advantageous practices, that may be a prime target for us to explore in terms of developing statutory language to address that gap.

Those that are yellow where maybe there is a reasonable law from Nevada level but federal law doesn't cover it as well or there is a gap, may represent a target for the future. We are going to find ourselves in a target-rich environment when it comes to privacy language, statutory language so we are going to have to pick and choose which ones we want to go after. The whole notion of having a

framework is to be able to say we looked across these different things that are fundamental either benefits and/or consequences of privacy and as a result of a gap in the existing statutory language feel like this one would have the greatest benefit for us and for the citizens of Nevada if we pursue putting a statute in place.

With that, I'll draw your attention to the spreadsheet page and explain how this might be applied in practice. I will just give a nod to the complexity of the exercise because of the number of different statutes that are out there; how they are intertwined; the way language is used in NRS; it is not simply a matter of going where are all the privacy statutes and what do they say.

The way that I would envision applying this would be to take a look at a particular element such as surveillance, I will take surveillance since it's the first one, and this is the harm's page, there's another spreadsheet page that covers CPBR and FIPS; and then examine from the hierarchy, contractual obligations. Do we have as a common practice in contracts, a protection against the negative consequences of surveillance? Or, is that a type of contract language that is rarely found? I think that in most cases, surveillance isn't something that comes up in contract language between two parties.

We move higher up the scale, in a regulatory environment, are there mandatory requirements that protect an individual from surveillance and if not, is there something we could recommend from a regulatory perspective? For instance, in the HIPAA language, is there anything in HIPAA that protects an individual from surveillance or recording of that individual's activities?

Finally, we get up to the statutory language and really, this is where we start to slice and dice NRS. Do we have current statutory language that defines or otherwise prescribes some sort of protection against unfettered surveillance in Nevada? If we do, what statutes are those and how well written are they. If there aren't any, then we propose some. Can we look to federal statute that is either current or proposed for guidance? Can we look at international treaties and laws to see if there are examples of language that would otherwise offset a harm of surveillance in some constructive fashion?

I think what I put down at the bottom is the notion of exemplars. We may be able to take guidance from other states in the way they crafted the legislation to address a particular harm or enforce a particular privacy practice and use that as an example for something we would like to do in Nevada. What the next step in this process really involves is trying to take a look at what we believe are the most egregious harms, the most beneficial practices and see where we have gaps in the language in the current statute, to see where there aren't current contract practices or regulatory practices to offset those statutory gaps. Then pick and choose the ones we think have the most benefit and build a strategy around starting to articulate language that would otherwise produce some

guidance from a statutory perspective to offset the harms and enforce the benefits.

That is the quick overview – any questions?

Jim Earl:
Not a question but just an observation – one of the reasons why that I think that any liaison with EFF would be so important is that that organization is likely to have done using their own terminology, a fair amount of the basic research that underlies this. I would view them as a fundamental source. The ACLU may be valuable as well; however, the ACLU is a much larger organization than EFF and the ACLU has a much broader scope of interests so when it comes to the ACLU, you really need to be able to find the right individual or the right group within the ACLU that would be focusing on digital or IT issues or whatever terminology they use to differentiate that from some of the broader ACLU concerns. The real benefit from EFF is that as their name suggests, they are already targeted on much narrower set of legal and regulatory concerns.

Jim Elste:
Hal has composited a number of example pieces of legislation or other synopsis of existing privacy laws that, once again from Jim's point, can serve as a basis for starting the process of trying to define what is or isn't a beneficial type of statutory language. I agree with Jim wholeheartedly that the EFF in particular has looked at this and I believe, actually published one of those synopsis.

Hal:
The fact that you selected surveillance as the illustration of how to use your spreadsheet, I think is timely because I was involved in the UAS project early on when it was initiated and so I'm somewhat familiar how that unfolded. At this point, Nevada is one of the five drone sites and I believe Governor Sandoval has appointed a privacy czar for the UAS project. I think he is a former reporter as I recall. This certainly is timely that you used that as an example because we are one of the five states that digital surveillance is going to be even increasingly more important for us to deal with on a statutory basis. Is this something that we should be pursuing in the short term? It is something we can add to our list of discussion items?

Jim Elste:
I think you hit on an interesting application of the taxonomy because surveillance in and of itself, is a very well understood harm. Nobody feels particularly comfortable with excessive amounts of surveillance. It's both pragmatic in the sense that people understand viscerally the harm associated with surveillance and as you point out, it's timely because we are seeing technologies like drones that propose to, in some respects, change the playing field from a surveillance perspective. The interesting part about this is not a zero sum game. It is a matter of balancing the harm against the benefit so while surveillance drones

have a distinct benefit in certain contexts, I don't think we want them necessarily circling our houses. How do you get the right composition of what something from a technology perspective is doing and what the benefit is in offsetting the potential harm and having something like the taxonomy to ground the focus of that harm? The old adage Supreme Court Justice Brandeis used when describing privacy as the right to be let alone doesn't really help us in looking at what we need to explore from a strategy or from a statutory agenda when it comes to privacy so my sense is that what we have in the taxonomy is some very visceral, very easy to understand privacy harms and then on the benefit side, things like transparency, things like having no secondary use of our information become very easy to understand aspirational objectives for privacy. As Hal points out, it becomes a matter of is there something happening, like the drone program, that brings one or more of those harms or one or more of those benefits into sharp relief and absent some explicit language, requires us to explore some sort of statute or otherwise define an expectation around that. We have a target-rich environment. There is going to be a lot of interesting work done by this subcommittee. There is no shortage of opportunities.

I would point out one other thing – the header on this page says IDESG Privacy Committee. Part of the genesis of this framework is the work that I was doing on the IDESG with the evaluation methodology reproduced for works of the IDESG so being one of the co-authors, I co-opted a bit of that to build our framework. I will get that corrected in the subsequent version.

Hal:
This suggests something to me. Brett, do you know the privacy person that Governor Sandoval appointed to the UAS Committee.

Brett:
No, but I will follow up and find out.

Hal:
I would like to suggest something to the committee for consideration. Would it be useful for us to invite him to our next in person meeting and ask just what they are doing to protect privacy.

Jim Earl:
Yes, I think that's appropriate. I would expand a little bit on the purpose of his participation however. Practically speaking, it seems to me that one of the dangers of government work is that particularly in areas where there is a new entity that is created, there's a tendency for that new entity to believe that they are the sole interest focusing on a particular concern. Very often, because many of these people may be new to government generally, they are unaware of the way in which to tap into existing government resources. I think that by establishing some sort of contact with the privacy person in this particular drone initiative, we should not only ask what they are doing but also should volunteer to

share information with them. If I were the person who was newly appointed to that position, I'd be looking out over a national landscape that has some states that have essentially passed legislation embodying a shoot down right for individual citizens when drones encroach or fly into the airspace above their private property. In that type of environment, again, if I were the newly appointed person, I would be scratching my head the first week or so wondering what I'd gotten myself into where I'm supposed to design a program where I realize that forces in other states have coalesced around a model that would lead to shoot down of valuable assets that I was trying to explain and justify in a privacy forum. My suggestion, generally, would be to approach this person and simply at the very outset to identify ourselves as a potential resource that he might find useful because this person may be called upon in the next legislative session to defend against the legislator who wants to enact a drone shoot down statute in Nevada. If he is able to say I've talked to the Technical Privacy Subcommittee of the Tech Crime Advisory Board and had active discussions with them about how to protect citizens rights in states from drone surveillance then he has an appropriate response to some very obvious legislator questions. I think that maybe this won't be immediately apparent to this person but upon reflection, we share some common interests and can potentially scratch each other's backs in areas of concern to both of us.

Hal:
As I understand it, you are suggesting that there is a response that he can offer to the Legislature that would be more satisfying than one that shows that these drones have been weaponized.

Brett, could I ask you, do you know this fellow, he is a reporter.

Brett:
I do not but I believe the State has established a drone working group.

Hal:
Yes, I was part of it. Stephen knows virtually all of those major journalists in the state and I thought he might already know. Brett, can I give you an action item to find this person's contact information and pass it on to me so that I can reach out to him and initiate the discussion.

Brett:
I am trying to look it up as we speak.

Hal:
We can handle that offline and send an email so that we can move on.

12. Discussion and possible action on report to Technological Crime Advisory Board and Technological Privacy Subcommittee findings and recommendations.

Hal:

That was my action item. Brett, how quickly could you get me minutes for this meeting? [Brett: Next week]. I have to be out of town but I will type something up on the road and send it to you and failing anyone else that needs to do it, Brett , you can present the summary to TCAB. [Brett: Certainly].

13. 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.

Hal:
That was Jim Earl and I. I must confess, I forgot to get in touch with Jim Earl on this. Do you have any further thoughts, Jim, about the joint resolution?

Jim Earl:
Just a little bit of background, this essentially arose out of a discussion you and I had about whether it was realistic for us to do something in state law or to try to effectuate some sort of change at the federal level. One of the things that we did come up with out of that conversation was that perhaps the most effective way to play this, independent of direct lobbying to individual members of Nevada's congressional delegation, would be to come up with some language in a joint resolution which would be broadly acceptable so that the Nevada Legislature would pass a joint resolution that would essentially ask the Nevada congressional delegation to support the issue of concern to us. Clearly, there are a number of different hurdles there, not the least of which is getting something that is both meaningful and broadly acceptable enough to be accepted as a joint resolution at the Nevada Legislature. I think it's a worthy issue to approach and one of the ways in which to move towards that is to broaden the set of legislators that are exposed to whatever idea we happen to have. Right off the top of my mind, because of the way in which one of our existing statutes are written, there are at least three groups of potentially concerned legislators. There are the two legislators who sit on the Tech Crime Advisory Board; the two legislators that sit on the Information Technology Advisory Board and the two legislators that sit on the Nevada Homeland Security Commission, which is also a joint executive-legislative structure with two participating legislators. If we were able to craft something which then could be brought to each of those three groups of legislators and those respective advisory boards then that would provide a precursor to an important nexus of legislators sufficiently broad to give a joint resolution at least serious consideration. One of the ways that I would characterize the Nevada Legislature is that because they are part time legislators and legislative sessions are short, tremendous deference is often given to legislators who have background or expertise in certain areas as to whether something in that area is a good idea or bad idea. There is a broad spectrum of philosophical concerns when you have the Tech Crime Advisory Board on one end which would have one view of privacy and the potentially the Homeland Security Commission on the other end which would have a different view of privacy. If we were successful in getting those six legislators to share some

common view on a joint resolution then the likelihood that that joint resolution would at least receive a reasonable hearing before both houses would increase. I would suggest that we consider building that into any model that we have once we get something that we feel is likely to be generally accepted as an expression of principle. We run that by those six legislators, either formally or informally, incorporate any feedback that we get from them into a second effort before trying to move forward.

Hal:
That leaves us with a same action item for next time. I promise to get in touch with both of you to sketch out some sort of framework to present to the subcommittee for the next meeting.

Jim Earl:
I'm not sure we would introduce this in resolution text or whether just as background and this goes to the taxonomy that Jim explained in terms of hierarchy of regulation of state and federal laws. We need to come up with something that would work in principal whether it applied in state law or federal law. I think that's doable. We need to be mindful if we are going the joint resolution route, we have already accepted that the solution that is most appropriate is done at the federal level. We are asking the Nevada legislators to call on the federal contingent to consider introducing legislation.

Hal:
It is my recollection what triggered this was a general discussion of NSA surveillance, is that your recollection? That's the reason we thought something like this might be viable.

Jim Earl:
I'm sure that that was one of the precursors of our discussion. I'm not sure it was the only one. There a lot of things going on, for example, the fact that you can't cross an intersection on a street in London without being part of a surveillance video. It's totally independent of NSA but is a concern that exists, as is the controversy that has surrounded the ability to issue a driving ticket for having gone through a red light where the evidence is an electronic speed trap traffic camera. The entire traffic camera agenda and whether a state has those laws or has repealed them. They have enacted a traffic camera law only to repeal it. That's all part of the general background in terms of citizen concerns over privacy scope, both in terms of surveillance in particular but what consequences then flow from surveillance. A number of different things underlay our discussion.

Hal:
I'll follow up with you, Jim, on this so we can put something together for the next meeting. One comment I would like to make about this is that the video surveillance is in part in the United States handled a little differently than it is in London. In one example, Seattle installed at NSA expense some surveillance

cameras in the downtown area. It was all integrated wirelessly so not only did they have the surveillance camera at work, they would also authenticate with whatever wireless device you have on your person, they can get a sound association between a face and a MAC address. The problem that I had with this was that not only did they not tell the public, but they lied about it. I have an article on this surveillance on my website if you are interested, I have the details. The issue is this - when a reporter walked around downtown he noticed his handheld device authenticating with WAPs on poles and he asked the police chief why his smartphone is authenticating with your pole and your camera. That started a litany of lies. Here's a thought that I had, it seems to me in a very fundamental sense that that kind of deceit should be illegal.

[Group discussion inaudible]

Hal:
We don't deal with that in our statute as far as I know. I don't want to get too Clapperesque about this with the nuances like the "least untrue answer." The appropriate response was "I'm not going to talk to you about it" as police chief. That, I don't have so much trouble with but to lie to the public – with that I have a problem. We could deal with that in our statute so far as I know. Wouldn't that be something – that whole train of not being deceptive about the surveillance practices that the municipalities and the state has when enquired by the public -- Wouldn't that be a useful statute?

Ira:
This does go back to my earlier comment about informed consent but also more relevant here in Nevada, we have the expanded use of surveillance cameras especially on Fremont Street in Las Vegas and on Las Vegas Boulevard. I don't think that this is a theoretical conversation or situation. To the extent that we have surveillance cameras having transparency as it relates to privacy seems to be something the public would support. Even though members of the public would say, I don't care, then to have members of law enforcement or elected officials or appointed officials lie about the extent of surveillance. I think even the people who don't care about surveillance would not agree with that.

Dennis:
To extend the thought a little bit, an interesting paradox here. Surveillance cameras on Freemont Street are ostensibly for public safety. Making the public aware that there are surveillance cameras actually helps the public safety objective. However, the problem is not so much that there are cameras on Freemont Street, it is what is being done with the data that is being collected by those cameras and that's where we get into the mire of the limits on surveillance and the harm associated with it because in many cases, we do not know what happens with the data that is collected through the various surveillance methods.

To your point, Hal, we are sometimes lied to so it is a matter of just the act of surveillance but it is the purpose behind the act of surveillance and the use of the material collected through surveillance that really fully fleshes out the problem of surveillance.

Ira:
This directly ties in to an area that again, affects Nevada today and there is no clarity of the law. That is – what happens to vehicle license plates scanner data? Vehicle license plates are being scanned by law enforcement here in Nevada. We have no guidance or boundaries, no procedures, no process that I've been able to discover related to what happens to that data. How long is it stored, where is it stored, who can it be sold to and who can it be shared with? Why is it stored?

Based upon my research, it is just a check report of whatever that department wants to do that day. There is no statutory guidance that I've been able to find and no guidance that members of law enforcement that I have spoken with. When I asked what they rely upon, they said they didn't know.

Dennis:
The limits on public agencies have to do with costs. They don't store them because past a certain length, they can't afford to manage them because an evidentiary chain is required so there are a lot of administrative costs. We actually have fairly tight information deadlines where we would delete it. The interesting part about this discussion of the license plate reader is some of the earliest data bases created were on private property, such as some of the Las Vegas Strip properties in their garages. I have no idea what happens with that information or if there are any limits as to what they can do with it. They certainly would let us look through it and in fact, there was a public and private partnership where the place itself was queried through Nevada criminal justice databases and NCIC. There is a lot of that data out there and I agree, I don't remember any explicit directions in state of local law on how long we had to keep it, how long should be keep it or any of those discussions.

Ira:
I have done some research on this and this is an area in which the ACLU has shown interest. Not Nevada ACLU but some chapters on the east coast have shown interest in this issue so we might be able to get some help from ACLU in statutory help or rules around this type of data.

Jim Elste:
Dennis, you hit on an excellent point and that is that not always do we look at things like surveillance are we simply looking at law enforcement agencies or intelligence agencies or government agencies in general? We have to remember that privacy is a construct that affects private sector organizations that do the same sort of thing. The type of data they collect when you go to the store or

when you are walking in a private organization's building and they are collecting surveillance video or on the website. There is equally an interest in those practices in the private sector and what I fear is that when we talk about privacy is that law enforcement agencies in particular think that it's an anti-law enforcement type of perspective. And, it's not. We certainly want to strike the balance in privacy between the interests of law enforcement and the interest of the citizen and in many respects, the interests of businesses in the private sector. It's distinctly a balancing act.

Dennis:
I think you are right with the balance. An interesting anecdote on that is some of the most immediate value that I saw prior that the owners get out of these readers was solving traffic collisions where people would hit cars in their garage and leave without reporting it. That could be used in the civil recovery of damages more than it was in criminal investigations but to amplify what you said about this being an open area, there weren't really many restrictions on what the private property could share with you. Simply ask them. There was no ownership of the data, other than it was theirs and they would give it to us willingly a lot of the time.

Stephen:
I was going to bring this up as a possible thing to look into – Utah, perhaps a year ago, passed a law against the use by private entities of these license plate readers. Within the last week or so, Mike Cardon, a fairly big litigator from DC, has filed a First Amendment suit in Utah to try to overturn this law. His client manufactures and sells these license plate readers, principally to automotive repossession companies. Apparently, they amass a huge amount of data to the point that they say they have been consulted by law enforcement and asked questions. 39% of the time they can provide information so these things must be all over the place. They are claiming it's a violation of the First Amendment rights of this company to take the photographs which the law prescribes and to disseminate the information which the law also prohibits. The Utah law is pretty straight forward – it says that no one can do this except law enforcement and parking agencies, essentially.

The problem there isn't the public photography of license plates which ostensibly is a sort of legal act under the First Amendment. It's the combination of the data with the information that exists in the DMV system that gives you the details about the individual who registered that license plate. Once you combine that data, now you've created something that ostensibly creates a privacy violation for that person. It's why this is always such a difficult thing. It's not just the surface act of photographing a license plate; it's the combination of the data. The power we have with the technology and the subsequent dissemination of that combined data that becomes a little disturbing from a privacy perspective.

[Group discussion inaudible]

Ira:
Aren't digital camera license plate readers infrared so they are not affected by light?

Dennis:
Some are, some aren't. A regular digital camera has an IR filter.

Stephen:
It does seem to be instructive about how we need to think about building statutes here in Nevada. We want to be careful that our statutes are more explicit about the privacy issue they are trying to address and not something that could be overly large or encompass things like digital cameras by inadvertently using the language that doesn't draw the lines clearly. That way, we avoid First Amendment lawsuits and the like. As we start seeing privacy statutes written in other jurisdictions, those are opportunities for us to examine both the issue that they are trying to address, the way they are trying to address it and then consider our own strategies for trying to address those issues to avoid either the consequences they are experiencing and their potential problems with the language they've chosen.

Jim Earl:
Since we are approaching the end of our agenda, let me bring this back to where we started. One of the first things how you asked about was a question that Brett answered about the Nevada Constitution: regardless of whether you have something in or not, one of the other sources of laws, not statutory law, comes through court decisions. If we use the example of the Utah statute that was just explained and look at that as an example where, unknowingly, a state legislature tried to be too prescriptive. Thou shall not do X without realizing how broadly X actually applied. One of the things that we may seek to do is either at the constitutional level or the statutory level, articulate some type of broad principles or set of principles which would then be available for court interpretation. That, in the long run, may be a more effective way to move forward than have to deal with an attempt to fine tune statutory language. Clearly, the Utah legislature spent a great deal of time with the drafters of that particular provision. They spent a great deal of time trying to accurately describe what a traffic camera did. Obviously, without realizing and in so doing, they were also describing what a smartphone camera will do. That suggests to me that we, at least, need to take into consideration a broader statutory approach that articulates principles rather than trying to define a narrow list of "Thou Shalt Nots" because the scope of what we think as a narrowly defined "Thou Shalt Not" may be more expansive either now or in the future than we think.

This is just a consideration to take into account when we look at either how we draft statutory text, whether we do constitutional or statutory text and also it goes to what we might reasonably seek to include in a joint resolution proposal.

XXX: 33:31
Mr. Chairman, I was just going to urge consideration of the full spectrum, too. The opposite end of the focus from defining all this specifically, encrypting next it was mentioned earlier is full disclosure. It might be an easier short term gain and simpler overall as a principle if all these captures of information at a minimum will be required to be disclosed at the point of capture, to the fullest extent possible. Thinking about a police officer in Nevada, in the absence of some specific ruling otherwise, all records are public. It would be nice if surveillance, any kind, private or public in Nevada, had a similar starting point where all that information can be captured in the absence of prohibition but it has to be that the people that are under surveillance get notified. It can be something as simple as the strobe lights that Metro puts on their cameras downtown or it can be more sophisticated but it's easier to do than trying to define, like Utah did, all the things you are not permitted to do.

Hal:
I think this has been a useful discussion. Ira, you brought up this topic – would you be willing to take on an agenda item for next time and compose a first pass at how one might integrate transparency and full disclosure and protections against deception when it comes to surveillance. If you did that, in parallel with Jim and I trying to come up with some framework for a sense of the legislature, we might have a convergence that would be useful to us.

Ira:
As a non-attorney, let me call and reach out to some experts that I know to gather some information. As a non- attorney, I don't know if I am above my weight to write statutes but certainly to find information and maybe there are some model statutes or model language I can find.

Jim Earl:
Even just a conceptual approach is really what we are looking for. Sometimes, it's easier to express an idea in actual statutory language but often times, it's not. Whatever makes sense to you.

Ira:
Yes, then with that caveat and understanding, yes.

Stephen:
I wonder, too, and I'm not sure this is an issue for us or an organization like the ACLU or someone like that, but it could be that law enforcement entities, for example, keeping this data for who knows how long, wouldn't be doing so if someone just asked how long you are keeping it. Just the very question itself

might be enough for them to say maybe we need a policy of five years or three years.

Brett:
I think Dennis mentioned there certain provisions that address the issue of retention of certain public record data.

Dennis:
The challenge that exists currently is now look at the NSA and some other agencies have gotten so good at metadata abstractions from the primary data, you have to be careful. If you don't keep my picture, but you but you keep information that it was taken at this location, on this date, you have a lot of information about me that has nothing to do with the primary photograph you took.

Ira:
I will add metadata to that. As a person quite familiar with digital forensics, I am quite capable of putting this in the context of encapsulating metadata into the issue. That's an excellent point regarding metadata.

Hal:
Because that's the easy way for a smart detective to say "I didn't break that rule, I just used this and that showed up with these other sources."

Ira:
Absolutely, metadata gives context, it allows misinterpretation of context, too, and so it's very important.

Hal:
Collecting all of this data is an invitation for blackmail. It's just a matter of time. Remember one date point: 75% of the NSA's budget goes to contractors. They are the ones who are harvesting the surveillance data and storing it. As we saw with Mr. Snowden, sometimes that stuff leaks. It's just an invitation for a lot of bad things to happen. If you don't have transparency, protections against leakage, it can lead to everything that Ira talked about

Since we are short on time, I will ask for any last minute comments.

Jim Earl:
Linked to what you just said, it's appropriate that this group be linked to the Nevada Tech Crime Advisory Board. As you said, Hal, the types of data that are now being collected and stored are a treasure trove for today's digital criminals when they advance to the next stage. Right now, data exploitation hackers or cyber criminals are principally directed at what one might call a first tier economic impact which is direct withdrawal of funds from bank accounts or credit cards. When we store additional types of information that can be linked in a variety of

different ways, we are storing a present and future treasure trove for additional types of exploits that would take place where a monetary reward is a secondary or tertiary affect rather than the primary effect that it is today. In looking at the possible criminal activity that could be associated with currently collected data, we have to be thinking at least as far out of the box as the best generation of cyber criminals right now. Thinking what is the next level of exploitation that can be done with the data that's being collected today beyond the initial primary source of direct withdrawal from monetary accounts. End of my observation.

Jim Elste:
I have one observation and a couple friendly amendments to the minutes.
We didn't have a formal agenda item to approve the minutes which might be a useful thing.

Brett:
I apologize: I included them in the materials but failed to include approval of the minutes as an agenda item and thus approval will have to come at a later date.

Jim Elste:
I believe the XXX on page 19 was my statement. The acronym is NSTIC and IDESG is the other acronym, bottom of the page second line from the bottom on page 2.

15 & 16. Location and time of next meeting:

Hal suggested another in person meeting (video conference) two months hence, a Thursday in April. April 24th or 17th at 1:30 pm.

Hal: We are holding over 5 and 6 for Allen Lichtenstein. Strike 4; 7 will recur; Dennis – do you want to discuss your topic at the next meeting?

Dennis: I will leave that to your judgment. I will work on refining it some more but I think you did great with some of the other things we talked about today so we could move with it.

Hal:
If it's alright with you, I would like to incorporate what we've discussed today and take your revisions next meeting.

Dennis: OK

Hal:
Number 9 – Stephen, can we count on you and Allen to work together and talk to the Nevada Press Association and Brett will give you the contact information. I will work with Jim Elste on Number 10 and carry that over to the next meeting.

Jim – what do you want to do with 11 – do you want it on the agenda next time or should we use it as backdrop against our further thinking on the other topics.

Jim Elste:
Start to use if referentially in our discussions about things like statutory language or Ira brings forward his report on the license readers things like that. What we will see very quickly is that there are lots of opportunities to pursue different topics and that can provide context for those.

Hal:
Drop Number 11. Number 12 will be modified to reflect that I will have written something that Brett will report to the TCAB and the update will be what the TCAB told Brett.

Brett:
I was going to recommend that Items 5 through 10 – I've been identifying them as for discussion only for these first two meetings but you are getting to the point where you actually have some written, substantive proposals so I would like to identify those as potential action items for the future meeting.

Hal:
My sense is the closest we come to having something to bring to the Attorney General is the News Shield Law. We might want to think about that for next time to discuss Allen and Stephen's update and the following meeting we might want to vote on whether we take that to the Attorney General.

Jim Earl:
Yes, I think that's right. I think the timing makes sense given what I can recollect about the schedule for bill draft requests and the timing of their submission.

Hal:
13 we will carry over and we will add a new discussion topic from Ira that will include transparency, full disclosure, metadata, and protection against official deception with regard to surveillance. Ira will define how that takes shape on his own.

17. Public Comment.
Jim Smith, lawyer, Reno, Nevada, and I am asking about the data collection aspects of your committee that is, specifically, what do you do to collect records of crime against the elderly and identity theft and exploitation? The documents that we have found so far are the State of Nevada Fact Sheet which is done by the Legislative Counsel Bureau and then we have the State of Nevada Elder Abuse Reporting System [EARS], and we have the Elder Abuse and Mental Health presentations by the Sanford Center?. The data that is available for

exploitation – how is it used and what is the State of Nevada doing to protect seniors, primarily/ Are there other documents that I'm not aware of; collections of data sources pertaining to exploitation and elder abuse and identity theft for seniors?

Jim Earl:
I am speaking as a former Executive Director of the Technical Crime Advisory Board – one of the things I think you need to take into account or be aware of is that this committee and indeed the Tech Crime Advisory Board essentially made a conscious decision that it would not collect records or data. My predecessor on the Technological Crime Advisory Board back 7 or 8 years, held a contrary view. She and at least one of her staff members were active participants in certain criminal investigations that were ongoing now 10 years ago. The reason that I decided not to become involved in that business was to avoid exactly the type of difficulty you question suggests. The Tech Crime Advisory Board does not hold or manage or use criminal information or indeed, any other type of citizen information. I can say the same thing about this particular subcommittee of that group. I was very conscious in aiding the Board to come to that decision because we wanted as an advisory board to be able to direct citizen inquiries to the individual agencies that handle, collect and manage the data. We did not want to do any of that and we do not want to serve as an intermediary to them. While put in your question context, it is fair for there to be citizen interest suggesting that we as a subcommittee of the Tech Crime Advisory Board, consider and look at safeguards that the State has around the collection and storage and manipulation of citizen data, we the Technical Privacy Subcommittee and TCAB are not a data source. The question that you pose is best posed to the Nevada agency that does collect and store that type of citizen information. It is a fair question to ask us and TCAB as to whether we think we are taking appropriate steps to oversee the management of that data that's done on an agency basis. Does that make sense?

Jim Smith:
That's very helpful but what I am looking for is the appropriation of individual data of older and vulnerable persons. What steps is this committee taking to assist the Attorney General and the duties of the Attorney General to protect the vulnerable population?

Ira:
I don't understand whether you are looking for the actual data related to actual events or there was confusion in your question. It seems like there are two issues: data collected about the events or legislation or matters to help protect seniors.

Jim Smith:

I think the legislation is in place with 603A and 205 – we worked with Senator Raggio and Senator Titus to bring that in and it was part of "technology develops and the legislature later, later, later says we are going to have these things." I am interested in where the data is collected – am I hitting the two most important ones for elders?

Ira:
Let me clarify my question – where is the data collected regarding seniors in general? Or data collected about the crimes against seniors?

Jim Smith:
Crimes against seniors.

Brett:
I can only tell you, in my experience in reporting on the problem of elder abuse and exploitation or vulnerable adult abuse and exploitation, those crimes are defined in statute. I have referred to criminal justice data that is maintained at the Department of Public Safety's Records and Technology Division which is reported as you indicated through UCR and then the incident reports that the Division of Aging Services has to maintain as a result of carrying out their statutory responsibility to respond to reports of elder or vulnerable adult abuse, exploitation or neglect. Those are the two sources of information that I have looked to get data on the occurrence of those types of crimes whether it rises to a criminal level or whether it's an incident report, it is investigated by Aging Services. The only other comment that I was going to make is that everybody recognizes that whether you are talking about elder abuse and exploitation or you are talking about tech crime in general, whether it's targeted towards those populations or the general population, there is a lack of good data and there probably, to the extent there is data, it significantly understates the extent of the problem, the extent to which somebody is a victim of tech crime or if somebody is a victim of elder exploitation or abuse is significantly underreported.

Jim Smith:
I am mostly interested in what we call the secondary use where either there will be a legitimate access to Tier 1 data or information that is then used by another person to inflict damage. The draining of the bank accounts is an easy one but there are many others.

Brett:
You are looking for data on how often that occurs? The only data I am aware of is the data that is maintained by Division of Aging Services on their incident reports and the criminal justice data which is supposed to be remitted by the local law enforcement agencies to DPS's Records and Technology Division. Once again, I would suspect they would greatly understate the extent of the problem.

Jim Smith:
Thank you very much. I appreciate your courtesy.

Hal:
Thank you all. As a Chairman's prerogative, I would like to ask a very simple question of Brett. Is it possible for us to change the open meeting law so that we don't have to print hard copies, we can merely post it on a publicly available website and provide the URL on the public notice? Is that possible?

Brett:
I would only be speculating but my experience is that it would be a difficult proposal to see through because those requirements were recently enacted in response to the concerns of the Nevada Press Association and citizens about the lack of access to supporting material for meetings. Those requirements were recently enacted to address those concerns and better ensure that the public timely receives supporting material for public meetings. While they are somewhat onerous in the sense that I have to have hard copies of anything that is deemed a supporting material available for members of the public upon request, I think those requirements were enacted under the rationale that democracy isn't always efficient and transparency in government sometimes creates burdens that we just have to bear. You could always propose an amendment to that. I know there's an Open Meeting Law Task Force that meets during the interim sponsored by the Attorney General that looks at open meeting law issues. It's from that task force that those requirements about hard copies of supporting materials were actually put into the open meeting law. I brought up some of those issues with them. New issues have arisen about the whole issue of supporting material – what is not supporting material, when does it come within the scope of the law that that group is trying to work through.

Hal:
As a computer scientist, I'm only interested in the dissemination of information. My recommendation would be "Think Green" so what has to be has to be. Thank you for doing a wonderful job of organizing this meeting. I want to recognize you for this so thank you very much for all the work you've put into the subcommittee.

Ira:
I would like to make a motion to adjourn.

Jim Earl:
Second.

Meeting adjourned.