TECHNOLOGICAL CRIME ADVISORY BOARD
Technical Privacy Subcommittee

MINUTES OF THE MEETING
July 31, 2015, at 1:30 PM

The meeting took place at the following locations:
Office of the Attorney General, Mock Courtroom
100 N. Carson Street, Carson City, NV 89701-4717
and
Office of the Attorney General, Grant Sawyer Building
555 East Washington Avenue, Suite 3315, Las Vegas, NV 89101

1. Call to Order and Roll Call.

Mr. Berghel called the meeting to order and roll was taken. A quorum was established.

Subcommittee members present:

Hal Bergel, Chair
Stephen Bates
Dennis Cobb
James Earl
James Elste
Allen Lichtenstein
Ira Victor

Subcommittee members absent:

None

Attorney General Staff Present:

Brett Kandt, Special Deputy Attorney General and Executive Director, Technical Crime Advisory Board
Laura Tucker, Deputy Attorney General
Lucas Tucker, Senior Deputy Attorney General

2. Public Comment. (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. Kandt thanked Laura Tucker for covering for him at the May 8, 2015, meeting of the Subcommittee while he was presenting a bill at the legislature.

3. Chair's Welcome. (Chair)

Mr. Berghel welcomed the subcommittee members and a guest, Senior Deputy Attorney General Lucas Tucker, who was attending the meeting in Las Vegas.

4. Discussion and possible action on approval of May, 8, 2015, meeting minutes.

Mr. Berghel suggested that it be noted in the minutes that this is not a verbatim transcript and may contain summaries.

Mr. Kandt stated that they could certainly do that, but as a matter of course, minutes are not presumed to be verbatim, as opposed to an official transcript.

A motion was made by Mr. Earl to approve the minutes. Mr. Victor seconded the motion. The minutes were approved unanimously.

5. Discussion of the following bills listed on the Nevada Legislature website for the 78th (2015) Nevada Legislative Session. (http://www.leg.state.nv.us/Session/78th2015/):

A. AB 179 – Revises provisions governing personal information.

Mr. Victor commented that there were a lot of edits and revisions to this bill. This bill amends NRS 603A. It's likely that come the next session, there will be interest in further revising the statute. He reminded the subcommittee that NRS 603A, which was authored by Mr. Earl, covers breech notification and safe harbor provisions for personally identifiable information (PII). It is reasonable to assume that there will be further discussions in the 2017 legislature to keep NRS 603A up-to-date. Since, Mr. Victor, Mr. Earl, and Mr. Elste have the braintrust behind NRS 603A, they may want to advise the Attorney General's office if there are revisions that they are hearing.

Mr. Kandt asked for clarification. Did Mr. Victor think that this committee should look at proposing further revisions to the statute?

Mr. Victor stated it was reasonable to expect that there will be demand to have further revisions in 2017. So the subcommittee should keep its finger on the pulse.

Mr. Earl added that given the testimony, and given the people who participated in the working groups during the legislative session, it is highly likely that a legislator backed by particular interests would propose additional revisions.

Mr. Victor stated that was correct. Revisions to NRS 6013A is probably something they should keep on the list.

Mr. Earl reported he had spoken with a couple minor employees in the IT community about that, and they have expressed the view that IT personnel need to be aware that the scope of information that needs to be protected in a particular way has been expanded. It would be appropriate to transmit that through the IT Security Committee, but that doesn't necessarily mean the information flows upwards to policy and records management individuals. Even if there is a significant change to an NRS, there is likely to be an operational lag in terms of agency action to recognize and implement additional protections around a broadened class of protected information.

Mr. Kandt asked if there was something he could do, like a memo or a summary, to help push out that information. Mr. Earl thought that it would be helpful for a memo to go to the agencies' Deputy Attorneys General so they could advise the principals that the scope of information has been expanded and their records need to be protected.

Mr. Kandt suggested the subcommittee develop something a little more specific as to how the things have expanded, and the basic impact. He can push out the information beyond the State level to all the district attorneys and local governments. Mr. Kandt asked for the subcommittee members' assistance in crafting the memo or summary.

Mr. Victor stated that when Mr. Elste arrived, they could come up with a plan. He added that come October, there is a change in the credit card rules under the payment card industry (PCI) standard that all government, public and private entities must follow and it is very parallel to NRS 603A in protecting personal PII. It might make a good memo covering the expansion in 603A and a reminder about the credit card rules.

Mr. Kandt asked what the effective date of AB 179 was. Mr. Victor said there was a delay. He believes it is July, 2016. Mr. Kandt proposed that since there is

a little time, they add this topic to the subcommittee's agenda as an action item. If the subcommittee creates a memo for broad dissemination to all affected government stakeholders, Mr. Kandt will be responsible for disseminating it. Mr. Victor thought that he, Mr. Earl, and Mr. Elste could help craft something. He thinks it is good role for the Attorney General's Office and that people will take it seriously, as they should. The whole purpose of NRS 603A was to give businesses and government agencies guidance on how to properly protect information, so they can avoid big, embarrassing breaches.

Mr. Berghel thought adding this as an action item to future agendas was a great idea and suggested the three authors send a draft to the entire subcommittee so that everyone can offer their input. He does not think that the PCI provisions are really relevant to the Attorney General's Office. He added that it is important to remember that there's going to be pushback. The meanings in reworking were modest at best, but important. Even as modest as the changes were, there are businesses that are not going to be happy because they don't want to protect any more information. They have a hard enough job just protecting the information they have. He encouraged the authors to say something like, please be aware that protections of PII have been enlarged which will be a strong benefit to the citizens. He thought the authors should pedal softly to minimize a negative reaction.

Mr. Elste joined the meeting. He stated that, on the first read, the nature of the changes are somewhat benign but the explanation of what some of the things are, like a unique identifier, can be contextualized a little bit better.

Mr. Victor added that Mr. Berghel used the phrase that the "protections of PII have been enlarged." That language matches the intent. The protections of PII have been enlarged because of the concerns of the citizenry over the explosion of recent breach disclosures.

Mr. Earl said that there was an additional potential benefit. If there are going to be additional expansion efforts in the next legislative session, the subcommittee's efforts in the interim may make it easier to get something meaningful done from the standpoint of understanding records and the IT security risk.

Mr. Elste added that historically, in terms of the breach disclosure law, there has always been some sort of grand strategy to get data in motion and data at rest encrypted and to try and enhance the protection mechanism for types of data handling. Going forward, part of the strategy is to start the process of divorcing the notion of first name and last name from credentials when it comes to identity theft and breach disclosure laws. When a credential is stolen, whether or not the

name is included becomes somewhat irrelevant if someone can sign into a banking system, for example. Right now, those disclosures are predicated on a combination of your last name, first name, *and* those identifiers now enhanced in NRS 603A. However, your first and last names are not always combined with a biometric identifier or a password.

By putting the language in the way they did, Nevada capitalized on California's language with a few enhancements which were amenable to all the parties in the discussion. "Unique identifier," covers any kind of identifier, whether you choose to use standard sorts of user I.D. and password combinations, or whether you do something really novel. The same goes for access control. Language is used that can encompass things like biometric identifiers as an authentication mechanism. The way the law is crafted looks surprisingly like California's law, but with those little additions that make it much broader in scope than California's law.

Mr. Berghel asked if the Nevada law was referenced in Wikipedia. Mr. Elste said he believed that it was Wikipedia's Breach Disclosure page that calls out California, Nevada and Massachusetts as exemplars of legislation. For Nevada, it was the addition of the encryption language that distinguished Nevada from the other states.

Mr. Berghel stated that he is not a fan of Wikipedia but in this case, he will make an exception. He asked Mr. Elste to send everyone the link.

B. AB 221 – Enacts provisions regarding Nevada student data privacy and protection.

Mr. Elste observed that this was the bill that requires the disclosure of certain elements that would be advantageous to an adversary, such as what the data fields look like, where data is being kept, and the third parties handling this data. Although well intentioned, this bill missed some obvious weaknesses from a cyber-threat perspective and it may be worthwhile to reexamine it in the next session.

Mr. Berghel asked who sponsored the bill. Mr. Kandt said he believed it was Senator Kearns's bill. Mr. Berghel suggested that the subcommittee get involved and be prepared to deal with that.

Mr. Elste added that the law doesn't take into context what someone might do with information they are proposing to collect and make public.

C. AB 239 – Enacts requirements and revises provisions for unmanned aerial systems.

Mr. Bates reported that the bill passed. It terms of law enforcement use, it restates the Fourth Amendment requirements. It doesn't propose anything additional. It says the Department of Public Safety will keep a registry of Government UAS to the extent that money is available for this purpose.

In terms of individuals, there was a provision in the original bill saying people can't use it for any type of surveillance of one another. This provision did not make it into the final bill. What it now says is that you have a civil cause of action for trespassing if someone flies a UAS at less than 250 feet after you have told them not to do it again. There are various exceptions; one exception is if you have a business license in Nevada and FAA approval, and are using the vehicle for business purposes that don't unreasonably interfere with use of the property.

Mr. Lichtenstein asked if there was a distinction between Nevada businesses and businesses from elsewhere, who do business in Nevada.

Mr. Bates stated he believed the terminology was, "a business licensed in Nevada," but he was not sure how that was defined.

Mr. Bates noted that there are some entities that are incorporated but not licensed, such as nonprofits. They could not operate under this exception.

An interesting question left outstanding is whether the use of your property includes privacy. There could be arguments either way. The NRS doesn't address that.

Mr. Berghel posed the question, do we have the right to use our airspace any way that we want? For example, can you shoot paint balls into the air so long as they don't go higher than 450 feet, as long as the paint balls come back down on your property?

Mr. Lichtenstein said that what you can and cannot do is strictly a question of violating the airspace.

Mr. Berghel said there was nothing about this bill he likes. He was uncomfortable with the way this was proceeding five years ago when he was one of the founding members of the UAV committee before Governor Sandoval got the money for it. The idea at the time from the people, mostly in the North, who championed the UAV program, was let's do whatever we want and then get the

public on board after the fact. Mr. Berghel was concerned about the privacy of the citizens of Nevada, but no one wanted to talk about that. That feeling had been preserved through the passage of this bill. That said, he is not sure anything can be done about it. He asked the subcommittee if working on this issue was worth pursuing.

Mr. Elste said that both he and Mr. Victor were asked to give some input on the UAS bill. The bill was extremely long and extremely contentious. There were a lot of parties involved and so they didn't spend a lot of time trying to contribute to the effort this session. His take on it is that ultimately we need to separate the law enforcement use of UAS and the commercial or private sector use of UAS and look at those as independent exercises. When it's all thrown together, there are two distinct objectives and ultimately it was very convoluted as to whether those objectives were satisfied. The worry was that the way the language was structured on the commercial side, which was stepped back from quite a bit, would have almost crushed the commercial UAS industry in Nevada by constraining their ability to do certain things that would be considered a normal part of operating a manned aerial system. The subcommittee has just under two years to get ready for the next session and get with the bill sponsors to see if there is an appetite for refining or improving this. Mr. Elste said he was concerned about fostering the commercial use of UAS with a very distinct privacy component to it. If Nevada is going to be at the forefront of this industry, nothing should be done to constrain commercial application of UAS systems. At the same time privacy must be protected. He thinks this bill tried to do too many things with one effort and so what they wound up doing through a series of negotiations was essentially passing off many parts of the original bill in order to get it to pass.

Mr. Earl added that they should also be aware that within the last week, either Google or Amazon made a proposal to the FAA for a tiered structure for drone flights. Between zero and 200 feet above the ground would be allowed for use by private flyers. Between 200 and 400, or 200 and 500 feet, would be exclusively for commercial drone delivery. Both of those uses would be further limited relating to certain types of aircraft use. The drafters of the proposal had in mind recent drone problems that impeded some aircraft in California. Regardless of the altitude at which you are operating, there are additional restrictions not to impede aircraft, firefighting aircraft, news aircraft, etc. If the FAA acts on this proposal there is going to be some blowback in terms of the interplay between state requirements and federal regulatory agreement. The FAA will probably act on this issue with something provisional between now and the next legislative session.

Mr. Elste added that not all drones operate in the air. There are drones on the land and in the water as well. Writing legislation about autonomous vehicles would also include self-driving cars. The legislative process does not take into account what is going to unfold and this is especially true in technology where it unfolds very quickly. The concern over things like this bill is that you wind up redoing them the next session because something has changed in the industry or the FAA has come out with more guidance on UAS. The subcommittee has the opportunity to keep this on the radar for upcoming sessions so we can look forward and propose some good legislation in this space.

Mr. Berghel said he thinks the appropriate first step regarding these overzealous business interests between the legislation passed and adequate privacy protections is sounding like a minimally proposed Article 2, Section 2 of the Constitution of Nevada to add privacy. In his opinion, that is the starting point and the signal that privacy is going to be at the forefront as we approach any legislation. He thought perhaps Brett could talk to the Attorney General and see if he has any interest in adding that to his list and see where it goes.

Mr. Bates said a provision in the original bill is that a person should not knowingly and intentionally operate an unmanned aerial vehicle for the purpose of observing another person, or capturing a photograph, or otherwise recording another person, which is pretty straightforward. That sort of thing wouldn't seem to interfere with commerce, with Amazon delivery, or with anything else. However, this provision was taken out of the final bill.

Mr. Berghel said it is instructive that if we want to keep people from spying by saying if they use a drone for that purpose, it could violate the law. It could even be a byproduct of what they're doing, but if personal information or privacy is violated it should be against the law, whether you intended your drone flight to do that or not. This issue is fraught with problems. It is pretty upsetting legislation in his opinion.

Mr. Lichtenstein said in terms of privacy issues, there are already privacy laws that are in place. There is the question of consent and also whether the photo is being taken in an area where one has a reasonable expectation of privacy. It may not be. For example, it could be taken in an area that is visible from the street. It is quite possible that the reason the language was taken out was because it needed a lot more work.

Mr. Bates said those provisions were in there: both consent and a reasonable expectation of privacy.

Mr. Berghel said that before the legislation was considered seriously, the detail should have worked been worked out, and it wasn't.

Mr. Berghel stated that the subcommittee will keep on top of this.

D. SB 444 – Revises provisions governing civil actions.

Mr. Kandt stated that this was the bill revising the anti-slapp law and it did pass, though it underwent some substantial revisions. The feeling was we have one of the strongest anti-slapp laws in the nation. SB 444 proposed to go in the opposite direction. Proponents of the bill thought the current law was open to too many abuses.

Mr. Bates followed the bill through the house and said it was quite modest; just a few sentences but he wasn't sure about the impact of that. Mr. Kandt said his understanding was that it struck a middle ground.

Mr. Lichtenstein stated he was one of the people who testified against this bill before the Assembly committee. The bill passed did not veer too far from what was existing already.

Mr. Bates said he thought it changed "clear and convincing evidence" with "demonstrated with prima facie evidence." That seems to be the biggest change. The moving party trying to get rid of a case has the burden in determining whether the case was established on that level.

For those who are not lawyers or not familiar with the term, the standard of establishing prima facie evidence is a fairly low one. "Clear and convincing evidence" is the second strongest standard, below "beyond a reasonable doubt." That particular change from the original language of the bill is a significant difference.

6. Discussion and possible action on recommendations on issues previously considered by subcommittee, including, without limitation:

A. Proposed revisions to the statutory definition of "personal information" in NRS 603A.040.

This topic was covered under agenda item 5A. Mr. Elste suggested the subcommittee keep an agenda item for the guidance memo as well as looking at future legislative opportunities for divorcing last name and first name from PII.

B. Proposed legislation to prohibit Automatic License Plate Reader Systems in Nevada.

Mr. Bates said that there was litigation pending in Utah he thinks Utah dropped the law to avoid litigation. The law was being fought by the industry. He heard it was dismissed on uncertain grounds but not on the merits.

Mr. Elste stated that license plate reader systems are getting a lot more visibility in the press. The level of awareness around these technologies is starting to grow, which probably bodes well for looking at legislative efforts to quantify how those are going to be used.

Mr. Berghel stated he had an article coming out in a couple of weeks in the *Cutter IT Journal* that deals with the velocity of innovation and the point of the article is that it's irresponsible to innovate without including in the calculus the possible negative externalities. That is socially irresponsible. The article is written for IT managers and leaders. He does not believe the public has any idea how dangerous these things are. Maybe the subcommittee can do something about it. It is abhorrent that we allow this type of information captured and integrated with databases without any attempt to protect privacy. It's kind of like NSA captured metadata. If you capture all the metadata of your communications, you know an awful lot about a person, even though a name is never mentioned. Same with license plate readers, if you know a car has been and where it is going, you know an awful lot about the driver. This should be stopped.

Mr. Victor agreed and said that the general public is starting to become aware that when the government collects all this information, those databases become targets for attackers. If the information is collected and needed for some exigent circumstances, like a kidnapping, to the extent that the data is looked at and then discarded because it's not a match, then that lowers the threat of an attacker going after the database.

Mr. Berghel commented that the life cycle of bad ideas can have a very long gestation period. We can't afford to have them around for decades, and then wait for a calamity, and then wonder why nobody did anything. We are at the point where we should try to do something. He does not know how that kind of legislation could be crafted but it would be interested to consider.

Mr. Bates said it is principally private industry doing this. The auto repossession industry around the country has aggregated mammoth national database which they are happy to share with police. There are no retention limits on this information. It's all private. There is no warrant requirement because they are

happy to oblige. I am not sure, for various reasons, how we are going to stop them from gobbling up this information. It may be the best to do is require law enforcement to get a warrant before accessing it the information.

Mr. Victor said he knows for a fact that law enforcement is still grabbing these. In Washoe County, law enforcement vehicles are scanning license plate data and they are storing it. Private industry is also doing it. One thing that could be done legislatively is to treat this information as PII and have some encryption mandates on it so that when the network that stores it is breached, it is a much more difficult task for an attacker to get useful information.

Mr. Elste added that the problems we are facing with license plate readers, black boxes, UAS, etc. is that we are looking at the wrong end of the telescope. We are looking at collection means. The means are varied and are going to change and evolve. The use of them will be in ways we cannot predict. If we take a step back, all of those systems collect data that is then put into a database and then used in ways we have concerns about. We shouldn't be writing legislation and trying to address the problem at the collection end, we should try to address the problem at the aggregation and dissemination end of the process. If you are taking and collecting license plate data, it's not a matter of the collection mechanism, it's the fact that you have collected license plate data, that your aggregating it with more forms of data and that your disseminating it to law enforcement without a warrant or to other private industries that may have less than noble intentions. Legislation could be written that says, regardless of your mechanism, if you're collecting certain types of data and using or manipulating that data, here are your obligations in Nevada from a privacy perspective.

Mr. Berghel asked if this is something that can be incorporated into section NRS 603A.

Mr. Elste said ostensibly the answer is yes, because what we're doing is defining PII in NRS 603A. We are creating a mechanism defining this type of data, placing requirements on the disclosure if there is a breach, and defining the conditions of breach, although it's very vague. The problem would lie with the scope of definition. The fact that somebody flies over your property and takes photographs of you may or may not be a privacy issue for you. We need an approach that says here are the types of things that trigger privacy concerns. To that end the PII definition in 603A is a start. It's narrowly focused on PII but can serve as a model that can be used to define these other types of data that raise privacy concerns. In grappling with privacy, it's still hard to say, dogmatically, this is privacy, and these are the things that need to be protected, and this is how you do it. The problems we have with privacy are the aggregation, manipulation and

dissemination of data. Hopefully we have an opportunity to frame that out so legislators understand how to frame privacy into things like black box legislation and UAS legislation.

Mr. Earl likes that approach in trying to handle a number of specific incidents in a general way. Rather than try and deal with information that might or might not be collected by an autonomous vehicle separately, it would make sense to write a generic privacy statute in such a way that it would encompass new collection techniques.

Mr. Bates added that the license plate reader companies are saying they have the right to gather this information and to take photos in public. He spoke to someone who works for a company that does biometrics and he said his company has been discussing whether they have a First Amendment right to take those photos and interpret them and put them in databases, etc. It would be nice to address these kinds of technological issues in a unified way.

Mr. Elste commented that there may be a First Amendment right to collect the data, but there are causes of action for First Amendment violations in how you use the information. Even though you may have collected the information legitimately, there are limits to what you can do with it. The First Amendment arguments that these companies make sound good on the surface, but it's about what they do with that data once they get. If they combine that information, all of a sudden that data has changed. If you have a license number and know where that car has been seen, you now have a composite of someone's activities. That's no longer a First Amendment collection exercise. It is not cut and dried, you can or can't do these things, or it is or isn't a First Amendment protected activity. There are many shades of gray which makes it a tough problem. The problem lies in the types of things you can potentially do with data that hasn't been considered or people aren't aware of it yet. If people are taking a picture of your license plate, it can seem innocuous but the potential damage it can do to an individual and their privacy in combination with other data is off the charts.

C. Proposed legislation to require full disclosure when metadata is captured and retained by government entities in Nevada.

Mr. Elste stated he thinks about the metadata problem every time he reads an article saying that at the federal level they are getting rid of the metadata that has been collected, or that they're going to stop using it. Metadata is extremely valuable and will probably always be captured in some form. The notion of collecting metadata isn't necessarily the problem. It is the disclosure of that metadata or the combination of that metadata and analysis that triggers a privacy

concern. There are a couple of good principals of Solove's "A Taxonomy of Privacy" that are instructive. One of the principals is transparency; the fact that I am collecting data about you and I'm transparent about it and how I intend to use it. In many cases, collecting metadata isn't transparent. You could assume that one principal of transparency is that the collection of metadata should trigger a requirement for some sort of management of that metadata and some sort of restrictions on its disclosure. These would be the types of things you would want to look at in a statute or regulation around things like metadata capture. Right now there is a lot of data is being collected without a lot of effort or intent, which has created a lot of problems. There is a certain misconception on what the value of metadata is. Metadata is not just abstract data that has no value for identifying an individual and violating their privacy, it just takes a little bit of effort to combine it and synthesize it into something that does. Mr. Elste said he would advocate for quantifying what we mean by metadata and using that as a basis for distinguishing what metadata is relative to other data and highlighting how metadata could be potentially abused from a privacy perspective.

Mr. Berghel asked if this is something that can be folded into NRS 603. Can metadata be called PII?

Mr. Bates said he thought PII was strictly speaking about the identifiers and the identification of an individual. NRS 603A was expanded to include credentials on systems, which is a form of an identifier. Not all privacy violations are violations of identity. There may be an identity component to it but you can violate someone's privacy without ever really focusing on their identity per say. For example, if someone discloses medical records, the medical records themselves are not part of your identity. But that data violates your reasonable expectation of privacy because the type of data about you is something that you are sensitive to. Not everything can be lumped into the notion of PII. If 603A is strictly about breaches of PII, some of the things they are reaching for in privacy would either expand the scope of 603A and have it recast or would, by definition of 603A, just be excluded. Metadata is abstracted enough that it can't really be directly tied to the individual as an identifier, but it can be incorporated into other information that can be otherwise manipulated to create an identification.

Mr. Elste suggested looking at 603A as construct for privacy legislation in Nevada and then see what is the potential of expanding the scope of that and creating a framework model under 603A versus a complimentary piece of legislation that would cover everything that's not in 603A. There should be laws on the books that describe privacy in the use and collection of data and then referentially incorporate those into UAS bills or license plate reader bills, etc. But if we could say here are our omnibus privacy regulations in Nevada, regardless

of if you are collecting data, or analyzing and processing data, here is what you need to know about privacy in Nevada. That would be a simpler approach for the creators, consumers, and enforcers of laws.

Mr. Kandt reminded the subcommittee to be mindful of the timeframe for future legislation. The next legislative session does not start for another 18 months, but the time frames for getting legislation submitted are considerable shorter than that. The subcommittee should consider the time it takes to submit proposals to the Tech Crime Board for their input.

For any legislation that the Attorney General might carry, there are time frames imposed by the LCB. It will be about a year from now that Bill Draft Requests must be turned in to the LCB, which means the subcommittee should have any proposals ready at least a few months before that in order to give the Attorney General time to consider them for his bill package. The advantage to the Attorney General carrying the bill would be that the AG bills get heard and enacted, although they may be amended. If the subcommittee meets every two months, that only gives them about 4 meetings to develop something they are comfortable with before taking it outside this room.

Mr. Elste suggested capitalizing on an opportunity to socialize these concepts before bringing forward a bill draft. The AG, the legislators and other individuals should be sensitized to both the issues of privacy and the potential alternatives to resolving some of those issues. There might be a benefit in constructing a proposal that outlines what they are talking about and puts a little more context around legislation. Conceptually, the subcommittee can help them understand the privacy issues better and see if there is any appetite for the proposals. It could be as simple as a lunch and learn on privacy. He suggested getting some people together and having a conversation about privacy in a context that doesn't demand that they immediately decide whether they will take a bill draft request for that. The subcommittee has an opportunity to contribute as educators as well as contributors to the legislative process.

Mr. Berghel said he thought that was a great idea. However, he would challenge Mr. Elste that metadata is, and can be, an identifier. You only need to look to the first order of logic and the way that it works to figure out that if you approach this from the point of view of set theory, you take the intersection of a variety of quantifiers that define sets, it's not difficult to get the point where the set that is left is a single. That's an identifier. The description may be the person who is currently logged onto this computer system, or the person who currently in the car and that's his license plate. We have been hung up on likenesses. We need to train ourselves to get away from that. Identifiers are not necessarily related to

these likenesses or names. And the metadata can be one of them. It's not a necessary condition for identification. Mr. Berghel thinks that metadata is a lot more dangerous.

D. Proposed telematics black box legislation.

Mr. Elste said he hoped everyone had seen the news articles on the Jeep recall because somebody hacked a car while it was in motion. People are now taking advantage of and exploiting the black boxes in cars and finding out the security isn't in place for those types of technologies. The hackers were able to honk the horn, unlock the doors, and turn the engine off – all of the fears the subcommittee has described around the black box and remote control of an automobile were crystalized in that one event and it made the national news. This is an indication that we need to get ahead of the problem.

Mr. Berghel clarified that the hack of the Jeep is independent of the black box issue. The black box issue was a privacy issue. You are no longer required to plug the black box into the port under the dash. It's now built into the computer and if you're using OnStar, its available to GM so they can monitor how fast you're going, what your driving habits are, etc., which violates privacy. The reason Mr. Berghel brought this to the subcommittee was to find out if the State would be amendable to passing legislation that would prevent the installation of these black boxes without the owners' knowledge. California had such a bill and it was blocked; it did not get picked up by the legislature. We haven't done anything with this. There is a big push back from business. This is the standard neoliberal challenge of privacy expectations. Business doesn't want to be limited on what they can do with that data so they are fighting it tooth and nail. Mr. Berghel's assumption is if California can't get a bill like that passed, Nevada doesn't stand a chance.

On the other hand, the Jeep hack is a telematics issue, and those hacks have been around for 10 years. The jeep hack just curried the fancy of the mass media. The way it works is the computer works with a series of what we might call microinstructions. For example, ABS requires a whole series of microinstructions to pulse the brakes. Pulsing the brakes is just locking the wheel for a very small interval. If you do that often enough you can adjust the traction on all the wheels in an ABS system. So, if the feature of locking up the right front wheel is a microinstruction, someone can hack into the car computer and do it while it speeding down the freeway. This issue does not have the same kind of privacy implications.

Mr. Elste thought that was a legitimate distinction but observed that when things like this hit the mass media, and companies like Jeep recall millions of vehicles, you can count on someone standing up and saying we need a law to prevent this from happening again. He believes that telematics and black boxes for vehicles will become an topic of interest in regards to both privacy and security. When the media reports on something like this, the public gets excited about it.

Mr. Berghel said that is a negative externality of a rush to technology. When computers were first put in cars in the late 80s, no one thought about if car computers were amenable to the same types of abuses as the computer on our desks. This was never addressed by executives in the auto industry. Maybe they should have been a little more circumspect when they rushed this micro technology to the automobiles.
He noted that since RF does not obey property lines, you just assume that RF is going to be in this soup around the automobile and some of its going to be hostile so you use encryption.

Mr. Elste said that his fear is that the uninformed become more motivated to try and take action. And uninformed action on trying to resolve these problems is scary because it can only make it worse. He noted that there was also a news was a story about a guy who tried to hack a plane. He was able to take control of certain systems in the plane through the Wi-Fi network on the plane, but he did it while in flight inside that same plane. These types of things are going to pop up on the news and when they do, people who don't understand how a car is hacked or how a plane is hacked are going to demand new laws. He thinks it's great that the media is recognizing these are problems. We need to do things about it but we must do intelligent things. Black boxes are the kinds of things people worry about because they drive their cars every day.

Mr. Elste pointed to the piece of auto loan legislation from the last session. Auto lenders wanted to install black boxes on cars so that they can disable a vehicle if someone hadn't paid their car loan. They swore up and down that the technology would not be used if someone was driving. Ms. Tucker stated that this technology is already being used in Nevada and the question was not whether it could be used, but it had more to do with the legal contract used in selling cars. The two completely different issues were conflated and the debate and discussion about the black box issue was eliminated complete.

Mr Elste added that people are using these technologies in ways we never thought they would and these issues are starting to get on the legislative radar. This is an opportunity to get ahead of the information curve and help the folks involved to understand these problems better so that they are educated when

legislation is proposed and will be able to determine if things are a good idea or a bad idea.

Mr. Elste said there were some legislators that were for this kind of legislation and that they would be natural candidates to reach out to when there is a proposal. One of the legislators was talking about banning black boxes until we can write proper legislation.

Mr. Berghel agreed that they would be better off being proactive than waiting for written legislation.

Mr. Berghel added that we're all in favor of transparency, but there is another side to this and that's accountability. There is little evidence that there is willingness on the part of legislators to hold people accountable for the disastrous result from misuse of technology where there may or may not have been good intentions to begin with. For example, if an auto company disables a vehicle while it is traveling on the freeway, instead of when it is parked safely in front of someone's house, the companyr would be responsible for the consequential damages. But legislation would not be worded like that because the business lobby is too strong.

Mr. Elste said legislating technology is the last resort in making technology do what we want it to do without those negative externalities or consequences. The right place to engineer this is at the engineering phase. If you take the data on miles per hour and combine it with the disable features, so that if miles per hour is greater than zero, you would not be able to disable that car. Therefore, you built the technical control in to prevent anybody from maliciously or accidentally causing harm. But that toothpaste is already out of the tube. We're talking about legislation that puts in statute requirements or prohibitions on people's use of technology. If you don't get it right in legislation, then you're just stuck with it and you have to go back to the legislative process to correct it. The subcommittee can't necessarily fix the technical problems but they can get in front of them at the pre-legislative stage and try to guide things so that we get the benefits of legislation.

Mr. Berghel asked if the bill that allows car dealers to install black boxes passed. Mr. Elste said the boxes are already in use. This legislation was to quantify how and when they could be used but it got way off track and became more about how you craft a car loan in Nevada. His sense was that the bill probably wasn't going to pass as it was, however he is not sure if it was modified, or improved, or if it ultimately passed.

Mr. Berghel asked if at least require transparency was required. Mr. Elste said that if he understood the testimony correctly, the dealers who use the black boxes get a consent form and some kind of contractual agreement from the buyer when they issue the loan and when they install the black box.

E. Proposed revisions to Nevada Unmanned Aircraft Systems (UAS) Test Site Privacy Policy (available at http://www.nias-uas.com/content/nevada-uas-test-site-privacy-policy.

Mr. Kandt stated he thought this was a holdover from prior to the legislative session. He doesn't know to what extent AB 239 impacts the existing Test Site privacy policy. The whole purpose of AB 239 was to extend, establish, and

devise some privacy protections for UASs. Mr. Kandt offered to contact Mr. Cunningham from the Nevada Test Site, who previously spoke to the subcommittee regarding the privacy policy, to confirm that the policy must be revised to comply with AB 239.

Mr. Elste suggested offering them assistance with revising their policy, if they have not already done so.

Proposed revisions to Nevada Revised Statutes relating to noirware.

Mr. Berghel asked if there is any appetite at all for protecting ourselves against abuse. The problem is that at the federal level, it is not illegal to surveil someone with an RF device, but it is illegal to jam them.

Mr. Earl stated that although his understanding of the issue may not be current, he believes jamming is still a big deal and it does raise its head in Nevada. Nevada prisons would really like to jam inmate cell phones, either entirely or selectively, but can't even though some of them are in remote locations and the likelihood of possible interference from that jamming is essentially nil.

Mr. Berghel stated there wasn't much he thought they could do as a state.

Mr. Elste suggested that rather than just abandoning it, perhaps they should look for opportunities to incorporate aspects of the noirware problem into the other efforts they are working on. Instead of trying to build revisions to NRS related to noirware, it might be better to incorporate it into some of the other pieces. Average people, including legislators, probably would not recognize what noirware was.

F. Proposed legislation to require mobile device security solutions, including without limitation, "kill switch" legislation.

This agenda item was taken out of order.

Mr. Victor advised the subcommittee that there have been a number of reports that the kill switch has been implemented in other states that those who are familiar with mobile phone forensics have been bypassing the kill switches.

Mr. Kandt stated that this agenda item was referred to the subcommittee by the previous Attorney General because there was some proposed kill switch legislation. Mr. Kandt had already conveyed that the consensus of the

subcommittee was that trying to foist upon everybody a statutorily mandated technology solution was not the way to go.

There is evidence that the phones are still being stolen and being sold for parts or the bad guys know there are ways around the kill switch and still are able to monetize the phone.

Mr. Berghel asked the attorneys on the subcommittee if this was related to the Jones decision. It seems to him that if you slap a magnetic GPS tracking device on a car or monitor the progress of the car with license plate readers, you're violating the same rights.

Mr. Bates said that the majority decision said it makes all the difference whether you slap something on the car. Several of the Justices said that even if you're not slapping something on a car, if it goes on long enough, there's a Fourth Amendment issue.

Mr. Berhghel said that only thing agreed on was that sliding it onto a car was trespass. He thinks that is misguided.

We entered into this problem because we, as a society, are focused on likenesses as identifiers and that is misguided. We should have, at the time the constitution was written, taken Mr. Elste's and Mr. Victor's approach and discuss this in terms of identifiers. We've already had the discussion about the rights of companies and the rights of individuals. If you know a person's location in space-time, you don't need know what his name is. You can do whatever you want with them if you know where they're at. Mr. Berghel pointed to the example of RF signatures. We have very sophisticated heat sensing devices now that can get a heat print that is fairly unique. Maybe the challenge is to do what Mr. Elste suggested and try to get this somehow into NRS 603A with an extension of personally identifiable information that includes stuff like location or any kind of signature, irrespective of the level of technology. If we approach it that way, maybe we could get some traction.

7. Discussion and possible action on recommendations regarding encryption on Apple iOS 8.0 and Google Android and impact upon law enforcement.

Mr. Kandt stated there is significant concern on the federal, state and local level over the encryption function and the inability of law enforcement to obtain authority from the manufacturer to override the encryption function, even with a

warrant, when investigating a potential or actual crime. This is a very big issue. Mr. Kandt wanted to know if this body was willing to make a policy statement, or recommendation on a policy statement to the Tech Crime Advisory Board, that can then be communicated to Nevada's congressional delegation and other interested parties.

Mr. Elste said the timeliness of this agenda item is impeccable because on July 6, 2015, MIT's Computer Science and Artificial Intelligence Laboratory Technical Report was issued. This was in response to a debate with FBI Director Comey over back doors in encryption. The consensus of the best minds in encryption is that it is impossible to create back doors that don't inherently defeat the purpose of encryption. Mr. Elste will send the link to the report to Mr. Kandt and would like the link to that, or the document itself, to be published on the record for the Privacy Subcommittee.

Mr. Elste said that reasonable people will read what the experts say about the potential of putting back doors into encryption and will understand that it is not possible, technically, to do that.

Mr. Kandt stated that when you have a situation where a child is missing or has been sexually assaulted or murdered, and there is evidence on the suspect's or defendant's digital device, to allow the defendant to be the only one with access to that device is very problematic.

Mr. Elste said that the law enforcement argument is impeccable exactly as Mr. Kandt framed it, but law enforcement's needs don't marry up with the technical realities. In response to this well thought out explanation as to why back doors to encryption are not feasible, FBI Director Comey's response is "you're just not trying hard enough." Law enforcement has a legitimate interest in having access to encrypted data but the argument that we somehow subvert what is a very technically effective and proven mechanism to allow that to happen is not a fair argument. It's trying to force a political and social policy of law enforcement interests on a technical mechanism that cannot be perfected and still have back doors in it.

Mr. Earl said he would explain it a little differently. Law is enforcement is familiar with CALEA, an act that was passed that essentially requires network providers to allow law enforcement into their networks to capture data. At the time the act was passed, Mr. Earl had some doubts as to how it was going to be effective because it wasn't clear at the time that you could take an essentially an analog process, a physical wiretap, and there would be a digital equivalent to that. It turns out that there is, so law enforcement has lived with CALEA and its implementation into networks for 25 years. His understanding of the fundamental position about encryption is that encryption is fundamentally different from networks in terms of the ability to allow law enforcement legitimate but

surreptitious entry. You can open a network to law enforcement but the technology around encryption is fundamentally different. So it is a fundamentally different problem to allow a back door into an encryption implementation. A network construct around encryption does not allow, without compromising the encryption technology itself, the type of entry that CALEA requires from networks.

Mr. Berghel said from a policy standpoint, the frequent mantra of law enforcement is to take something like the fear around a missing child and build policies on it. Having back doors on the encryption of the phones affects every person on this planet. In a free society there are some things you just have to tolerate. You can't invade the private space of everyone to try and avoid an incident. It is constitutionally insulting to propose we circumvent the encryption on these phones for what might be one or two tragedies. Unfortunately, tragedies happen.

Mr. Kandt stated that he disagreed from the policy standpoint. It's not just about one or two isolated cases. An increasing number of crimes are being facilitated by using technology. There seem to be a lot of references to bulk data collection and that is a separate issue than access to data on a digital device pursuant to a search warrant, which requires probable cause as determined by a neutral magistrate. Those requirements under the Fourth Amendment have always been there. They have served prior to the dissemination of technology, and they still apply to you and your home except when there is a search warrant. Mr. Kandt can appreciate the technical conundrum in creating a back door, but he still feels that if you commit a crime, and evidence of that crime is on a digital device, then law enforcement, pursuant to the Fourth Amendment should have some ability to access that evidence.

Mr. Elste argued that it is a policy conundrum, not a technical conundrum. The technical side is well understood. He suggested circulating the MIT report, so that members and staff of the subcommittee understand the technical restraints a little better. What's important to Mr. Elste is that the subcommittee can help inform people around the state why back doors are not technically feasible. The appropriate thing to do is create other mechanisms that help law enforcement exercise its obligations in collecting evidence and recognize where the technical restraints exist that cannot be compromised. The technical realities of encryption are that they are elegant in their simplicity. When you encrypt a file, it is no longer the same file. That data is no longer that same data. That evidence is not evidence anymore because it is no longer the file that it was before. What we lose in this discussion is that when you put the data through an encryption algorithm it fundamentally changes the data at a bit level. The only way to get that file back is to run it back through the encryption process the other way to get to a human readable file, which is what law enforcement is looking for. So you've got this notion that because someone used this for committing a crime, its

evidence on their phone, but it's a bunch of ones and zeros that are encrypted. If you can't recompile it into human readable state, it's not really evidence.

The other reason it is important to educate people on this is that Director Comey did a rather large disservice for law enforcement when he suggested that they were concerned about the efficacy of encryption. When you telegraph your weaknesses to your opponents, they are going to take advantage of that. By saying that he gave a clear indication to all criminals that they should start encrypting their transmissions because the FBI can't do anything about it.

Mr. Kandt stated that in all fairness, he doesn't believe law enforcement brought it upon themselves. He's seen press releases and representations from the manufacturers touting this. The criminals figured out the advantages of encryption long before law enforcement said there was a problem.

What it all comes back to is who can get search warrant, which is law enforcement.

Mr. Elste said it's not that simple. You've created a technical feasibility for compromising that security and it doesn't require a search warrant to do that. It requires that technical mechanism to be there. Good guys and bad guys can take advantage of that technical mechanism.

Mr. Berhel wants to leave this on the agenda for the next meeting for further discussion.

8. **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 stated he would like to introduce a new topic for the next meeting. He has sent out a report and survey on state location privacy legislation. He asked the subcommittee to look at the document at their leisure and it will be discussed at the next meeting. It basically says you have a right to protect your location.

Mr. Elste said he took a quick look at the graphic that had their states and their efforts in this regard and it doesn't look like there is a lot being done.

Mr. Kandt stated it looks like California just passed full protection for location this year. If this is something that the subcommittee may want to propose for the next legislative session, now is the time to work on it.

Mr. Elste said it ties back into the license plate readers and the other issues the subcommittee has been talking about because it all ties back to location.

Mr. Berghel added that he is comfortable with using location as an identifier.

Mr. Elste reported that he was joining as of August 1st; he is joining the full-time faculty at UNR and will be teaching some IS classes working on some cyber security initiatives at the University.

Mr. Victor sated he would be attending at least two conferences including Def Con the following week.

9. Discussion and possible action on time and location of next meeting.

The next meeting was set for October 2, 2015, at 1:30 p.m.

10. Discussion and possible action on future agenda items.

This was discussed under agenda item #8.

11. Public Comment. (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.

There was no public comment.

12. Adjournment.

The meeting was adjourned.

Protecting "personal information", the credentials and identification we use to transact business, ~~and~~ to access financial accounts, or other online resources ~~online~~, is fundamental to preventing identity theft. NRS Chapter 603A – Security of Personal Information, recently amended by Assembly Bill 179, provides for the protection of personal information.

Who does the law apply to?

NRS Chapter 603A applies to all "data collectors." ~~defined in~~ NRS 603A.030 defines a "data collector" as "any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information."

The essential element of the definition is the reference to "nonpublic personal information," which is a specific type of data. Entities should carefully review the expanded definition of "nonpublic personal information," evaluate the type of information they possess to determine if they will be considered a "data collector" when the revised definition of "nonpublic, personal information" goes into effect. Data collectors have until July 1, 2016, to comply with the amendments in Assembly Bill 179, ~~as further detailed below.~~

~~Data collectors have until July 1, 2016, to comply with the amendments in Assembly Bill 179, as further detailed below.~~

What is personal information?

"Personal information" is defined in NRS 603A.040. ~~?~~ Personal information is a natural person's first name (or first initial), and last name in combination with certain data elements, if the data is nonpublic and not encrypted.

Since NRS603A was first written, technology has changed dramatically, and the types of data and so have the techniques used by criminals to commit identity theft have changed considerably. While social security number, driver's license number, and credit/debit card numbers continue to require protection, Assembly Bill 179 amended the definition of personal information to include driver authorization cards number, medical identification number, and health insurance identification number.

One of the most significant additions is section 1(e), which covers the personal information used to access online accounts. A user name, e-mail address, or any other unique identifier in combination with a password, security question and answer, or any access code (e.g. biometrics, one-time passwords) that would permit access to an online account are now included in the definition of personal information. For example, if an employer uses an

employee ID number (a unique identifier) and password to access the payroll system, that information would be considered personal information under the revised definition.

The definition of "nonpublic" personal information is refined by Assembly Bill 179 to include only publicly available information that is lawfully made available to the general public from federal, state, or local government records.

One of the most overlooked components of the definition of public information is the reference to encryption. By using encryption, as defined in NRS603A.215, the data is no longer considered "nonpublic personal information", while it remains encrypted. Encryption offers the greatest protection for the data and reduces the entities liability by effectively eliminating the personal information.

~~While most types of data set forth in the definition are fairly straightforward, Assembly Bill 179 added a new subsection (e) that may require further explanation. ELSTE~~

What is required to protect personal information?

NRS 603A.210 ~~and 603A.215~~ requires data collectors that maintain records, which contain personal information of a resident of this State, to have reasonable security measures to protect those records, to prevent the personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. Contracts for disclosing the personal information of a resident of this state must include provisions requiring the recipient to maintain similar reasonable security measures.~~ELSTE~~

NRS603A.215 requires a data collector to encrypt the transmission or transportation of personal information outside of their secure system, unless the data collector accepts payment cards, in which case they are required to comply with the current Payment Card Industry Data Security Standard. Transmission includes the transfer of personal information by any form of electronic, non-voice transmission, except facsimile. Transportation includes the movement of any data storage device containing personal information beyond the logical or physical controls of the data collector.

In return for applying reasonable security measures, NRS603A.215 limits the liability of a data collector. A data collector shall not be liable for damages for a breach of the security of the system if the data collector is in compliance with NRS603A.215 and the breach was not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees, or agents.~~NRS 603A.215 further requires that data collectors use encryption to ensure the security of the electronic transmission of personal information.~~

What if there is a security breach?

NRS 603A.220 requires data collectors to disclose any security breach "to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Disclosure must be provided "in the most expedient time possible and without unreasonable delay" unless a law enforcement agency determines that the notification will impede a criminal investigation.~~- Data collectors that have the required security measures to protect personal information in the event of a security breach can limit their potential legal liability.~~