TECHNOLOGICAL CRIME ADVISORY BOARD
Technical Privacy Subcommittee

MINUTES OF THE MEETING
May 8, 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. Mr. Berghel, Mr. Earl, Mr. Elste, Mr. Victor, and Mr. Cobb were present. Mr. Bates and Mr. Lichtenstein were absent. A quorum was established.

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.

There was no public comment.

3. Chair's Welcome. (Chair)

Mr. Berghel welcomed the Subcommittee members, legal counsel Deputy Attorney General Laura Tucker, 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 March 6, 2015, meeting minutes.

Mr. Earl made a motion to adopt the minutes from the March 6, 2015 meeting. Mr. Elste seconded the motion and the minutes were approved unanimously.

5. Discussion and possible action on recommendations on the following bills or bill draft requests 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. Elste reported that AB 179 has passed through the Assembly and Senate and is on its way to the Governor's desk for signature. He and Mr. Victor, with some

guidance from Mr. Earl, were involved in the crafting of the language for this bill. Assemblyman Flores was the sponsor of this bill and they worked closely with him to ensure that his intent to incorporate new language into NRS 603A was actually met in the face of some very strong resistance in changing the definition of personal information. The language that they settled on was modeled after California's newly updated breach disclosure law and incorporates some additional terminology that did not previously exist. The additional terminology has broader connotations and will cover more of the types of personal identifiers and credentials that are used in online systems. In particular, a component covering driver authorization card numbers and medical and health insurance identification numbers was added. Section E covers a user name, a unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

With the addition of key terminology, Nevada's definition of PII is now in line with the common practice of usage in the online environment. Mr. Elste reported that they are thrilled the bill made it through the process and is on its way to being finalized. Mr. Earl commented that there is pending cyber legislation at the federal level that seems to have a better chance of passage than in the past. Although he is not sure what the latest version of text says, some of the reports are that the legislation is likely to preempt state breach notification laws. Mr. Earl believes that the problem with this is not the preemption (although some of his colleagues believe that federal law should not preempt state breach notification laws.) Mr. Earl's concern is that what many people are describing as preemption by federal action, is not a total preemption. The modification of the statute at the federal level would change an FTC statute. The problem with that is that the FTC jurisdiction is large, but it is not unlimited, and that would leave states in the position of applying the federal breach law to those entities that are within the FTC's jurisdiction, and then applying their own existing breach law for those entities outside the FTC's jurisdiction. This potential problem arose a couple of years ago and Mr. Earl expressed his concerns to Senator Reid's office. He does not think it's right to expect state Attorneys General to administer and prosecute under two breach standards. If the federal law changes significantly, it may affect the scope of applicability of the changes made by AB 179.

Mr. Berghel asked what Senator Reid's staff's position was on this issue. Mr. Earl reported that they were much more interested in other changes he wanted to make to the cyber bill involving the ability of state institutions of higher learning to issue certificates for cyber center training, and to change some of the wording in the draft statutes to make sure that UNR and UNLV qualify as information centers for cyber threat and amelioration information. The original language would necessarily qualify NSHE institutions as such centers. Reid's staff was not quite as concerned about the breach law issues because they are harder to explain, and because it would affect Attorneys General and their staffs rather than the general public.

Mr. Berghel said he agreed that if the government were to set up such information centers, NSHE should be involved. He advised Mr.Earl that if it should come up again, Mr. Berghel is most concerned about standards to certify the value of such cyber initiatives. The subcommittee members discussed the issue of standards for students, teachers and programs.

Mr. Victor asked if there was an appropriate role for the Nevada Attorney General to speak out on the impact of the federal cyber security bill on the state of Nevada. Mr. Earl stated that what usually happens is that individual state attorneys general don't get involved; they look to their national association (NAAG) to put state concerns before federal legislators. Mr. Victor asked if there was a role this board could play in advising the Nevada Attorney General to approach NAAG in order to pass these concerns on to Congress. Mr. Earl stated that the record this committee is developing with two members of the Attorney General's staff is the appropriate way to bring their concerns to the Attorney General. At NAAG, Hedda Litwin is cyber counselor and is the one most involved in this issue.

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

Mr. Elste reminded the subcommittee of the discussion they had at the last meeting centered around publishing the types of records that were held, where they were held, and with whom they were held, which could create a sort of road map for potential hackers. It appears that the bill is moving forward, intact, with the requirement for publishing that kind of information. Mr. Victor says he thinks it may be too late to have much of an impact on this bill. Mr. Elste agreed and said he thought the bill was already being enrolled for the Governor's signature. He noted that the bill references a federal statute for defining PII. The definition of PII is not explicitly clear in that federal statute, which is the FERPA statute 34CFR99.3 which defines a bunch of different types of data elements which might be collected, but does not define what personal information is. Mr. Elste thinks that these issues will make the bill problematic to implement.

Mr. Earl stated that to the best of his knowledge, the records referenced in the bill will be stored on servers owned and operated by the Department of Education. The Department of Education runs its own small, not particularly secure, data center. They do not locate their servers at the state data facility with the physical and electronic security that a tier three facility provides. This is because Nevada has failed to act over the last 10 years to appropriately consolidate and effectively administer individual agency servers. And we may, unfortunately, see the consequences of that.

Mr. Cobb wondered if there was any opportunity in the implementation of this bill—since it has passed in its form—to be done in a way that at least makes it more difficult for someone who wants to use this information maliciously. In publishing an index of the data elements, for example, would there be a way for a front office

administrator to use euphemistic terms and still meet the requirements and, perhaps, construct the index in a way that doesn't give a one-to-one correlation for someone with malicious intentions.

Mr. Elste stated that would probably occur because different educational organizations are going to use different mechanisms for developing and publishing this information. There is not going to be a set standard for what needs to be published and how it is presented. It will be up to each organization how they want to construct that. In some respects there may be a disconnect between a database administrator, who has a detailed understanding of the fields and how those fields are related, and what ultimately that organization might choose to publish as a made-for-the-public consumable response to this statute. He noted that the Department of Education is required to develop a security plan. Perhaps part of their plan will be to move their resources to a more secure facility. He stated that the Governor could decide to veto this bill. If there was an avenue for providing the Governor with some insight as to why this may not be good bill, that could potentially be one avenue left open to the committee at this stage. Otherwise, some refinements may need to be made in the next legislative session.

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

Mr. Bates was to provide a report on this item. Since he was absent, Mr. Berghel asked the committee if they had any comment. There was no comment. Mr. Berghel asked that this item be carried over to the next agenda.

D. SB 444 – Revises provisions governing civil actions.

Mr. Bates was also to provide a report on this item. There was no comment by the committee members present. This item will also be carried over to the next agenda.

6. Discussion of status of previous recommendations by subcommittee, including, without limitation:

A. Proposed amendment to Nevada Constitution, Article 1 Section 1, establishing an express right to privacy.

B. Request for Nevada Legislature to pass joint resolution calling on Nevada congressional delegation to expand online privacy rights under federal law.

Mr. Berghel asked the committee if there was any objection to skipping agenda item 6 since the topics needed no further discussion and there was no action item before the committee. There were no objections.

7. Discussion and possible action on identification and prioritization of issues for consideration by subcommittee, including without limitation:

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

Mr. Elste reported that most of the work they had been discussing with regard to NRS 603A was accomplished with AB 179. However, he does think there is some future work to be done. He believes there could be better alignment between the use of personal information and personally identifiable information. It is also worth pursuing decoupling an individual's first and last name from identifiers. For example, if someone has a username and password, there is no need to know a person's name. A compromise of the credential would then be absent the name of the individual, subject to breach notification. But the passage of AB 179 is moving in the right direction.

Mr. Earl added that it is possible that a future definition of PII might involve simply listing a number of different attributes including first name and, separately, a last name, and other identifiers. The definition of PII might be disclosure of any two or more of those attributes. Use of attributes, not including a first or last name, may be sufficient to establish identity. That may be a way to modify future definitions of PII.

Mr. Berghel noted that you don't need to exclude any particular data sets because you can identify indviduals with rather obscure data sets. The problem will get worse over time and perhaps it is a topic the subcommittee can continue to explore.

Mr. Elste stated that Mr. Berghel's point was a powerful argument against weakening the security standards that have been articulated in NRS 603A. Encryption is very hard to crack. Deanonymizing data sets is not that hard to do, so using obfuscation techniques or deanonymization techniques to protect PII is also something to be on guard against because even in this last effort to change 603A, there were people proposing weakening the security standard they have in there, specifically the reference to encryption. The fact that you can de-identify someone with database manipulation means you can re-identify someone with a similar kind of manipulation. You need to be aware of how easy it is to combine data elements and identify a person in ways that can be harmful to them.

Mr. Earl commented that given the discussion, it is possible to look at any breach notification law, and any definition of PII as nothing more than a way to provide the citizenry with a false sense of security. Citizens' identities are at risk simply because of the multiplicity of data sets that now exist in the wild. Any modification of PII and data breach laws is likely to be ineffective in safeguarding citizens from misuse of their personal identities. Changes to the law do nothing to reign in information that is already on the loose.

Mr. Berghel commented that the South Carolina Department of Revenue act is an example of how a government can do everything wrong and create mayhem in terms of the citizen's right to protect themselves from identity theft. They are spending something like five-million dollars into insurance to cover the cost of citizens' loss of PII, which is far more than they would have spent defending the servers that contain the information. Perhaps this is the message that should be extended to the state IT department, and to anyone who will listen.

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

Mr. Berghel deferred discussion of 7(B) because Mr. Bates was not in attendance to present information.

As a point of order regarding the agenda, Mr. Elste commented that it would be better to avoid using the phrase "to prohibit" as is in agenda item 7(B), and simply talk about legislation around those issues. "To prohibit" sounds like a forgone conclusion. He thinks "regulation" or otherwise addressing the issue associated with that would be more appropriate.

Mr. Victor suggested the word "manage" might be more appropriate when discussing data types.

Mr. Elste thought item 7(D), "Proposed telematics black box legislation" was a model way of writing an agenda item. It is neither pro nor con, and has no qualifiers on what type of legislation. Mr. Victor agreed that made sense.

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

This item was not discussed.

D. Proposed telematics black box legislation.

Mr. Berghel said that this was a topic that he brought up. It was never clear whether the committee would be able to do anything about it. He noted that the California bill was not passed. He asked if the subcommittee members had any information on this topic.

Mr. Elste stated that there is currently a piece of legislation in Nevada relating to the use of telematics devices for auto loan providers as a mechanism for doing electronic repossession of vehicles. They are normally installed on used cars sold to sub-prime or high risk borrowers to monitor the location of the vehicle and

to disable the vehicle if necessary. The bill in front of the legislature proposed some regulation around the use of these devices.

Mr. Elste noted that there are a variety of applications of this type of technology the committee may or may not be aware of, and there is legislative activity around questions like this that may or may not, on the surface, appear to be directly related to the topics as the committee discusses them but are highly relevant. He suggested finding out the status of this particular legislation and incorporating it into future discussions. If the bill passes, it could be a starting point for embellishing or broadening a telematics black box type of legislation. He said he would find the information and send it to Mr. Kandt so it can be included on the next meeting agenda.

Mr. Berghel asked if OnStar was being used for this. Mr. Victor said he and Mr. Elste attended the first session of the Assembly where this bill came out. As it was described in the hearing, these are stand-alone ignition interrupt devices. They do not tie into the existing telematics that are on the vehicle. According to the advocate for the bill, they combine GPS with ignition interrupt so that the vehicle can be disabled when it as at someone's home. The proponents say it would not be activated when someone is away from home with the vehicle, but only when the vehicle is at or near the residence overnight and the individual is presumed to be safe at home. Mr. Berghel commented that if the system is not part of a satellite system like Onstar, then it has to be RF, which is hackable. Turning off a car in the driveway is just one hack away from turning it off when it is on the freeway. There are vulnerabilities that the car owner may not be aware of.

Mr. Victor advised the committee that the biill in question is AB 228. He described the testimony of a young woman who bought a car with this technology and who claimed the car ignition cut out on the I-15 freeway in Las Vegas. Advocates for this technology say that's impossible. They say once the car is started, the technology will not interrupt the spark getting into the engine. However, there were a lot of gaps in the testimony on this bill. Testing of the system, including security vulnerability, was not discussed.

Mr. Elste looked it up and said that AB 228 was voted down in the Assembly on April 20, 2015.

Mr. Berghel would like this topic included in the next agenda.

Mr. Victor noted that the failure of this bill does not mean that this technology is not in use. The bill was to change some of the lending regulations that would potentially impact the use of the technology. This is still a very active subject and an appropriate place for this committee to provide guidance for the Attorney General for future legislative sessions.

Mr. Elste added that there are two components of this bill. One is related to how contracts are structured in auto lending. The other is about the telematics being unregulated and is being used without any sort of statutory requirements, sometimes in a potentially coercive fashion, such as a condition of getting a loan. In a future legislative session, it would be better to separate the telematics component from any sort of contractual language when getting an auto loan. He suggested studying the bill to see if the committee could get any insights for the next session.

Mr. Cobb wondered what the actuarial value would be of having a large data set of locations where people with a bad credit risk drive or park their cars. He wondered if there were any restrictions on personal information generated by tracking somebody already identified as having a bad credit risk and ways it would affect access to credit. It is all interconnected.

Mr. Victor stated that according to the proponents of this bill, they take privacy concerns very seriously and have policies in place to protect the privacy of the drivers, but they offered no specifics in the testimony he witnessed. They also claim that they do not record the information around GPS tracking until someone is late in paying, but they did not specify the audits and controls around that.

Mr. Berghel said that there was no question that this is a huge area of vulnerability for the citizens from a number of perspectives.

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. Berghel stated he would like to hold off on this topic until Mr. Bates can attend, but asked the committee members present if they had anything to say. There was no discussion.

F. Proposed revisions to Nevada Revised Statutes relating to noirware.

Mr. Berghel stated that he had published on this topic and said that as far as he can tell, there is not a lot that one can do defensively that doesn't violate FCC rules. He asked if there was much the state could do to regulate Noirware?

Mr. Earl said there was not, insofar as it involves frequency regulation. Jurisdiction over RF falls to the FCC for commercial use and NTIA for government use. Those two federal bodies preempt state regulation.

Mr. Berghel said he does not want to give up on this yet as it is becoming a huge problem with such things as RF trackers, GPS dots, and GPS spoofing. He would like to carry this topic forward and will, perhaps have something more to say at the next meeting.

Mr. Earl said that Homeland Security, at least at some level, has begun to realize the problems associated with spoofing of GPS information. He read something that said Homeland Security recognizes that a terrorist group could locate a ground transponder that would spoof either a satellite GPS signal or would spoof a legitimate augmentation on the ground of that GPS signal to put a plane down in bad weather two miles off the runway. Mr. Earl was unsure whether there has been any attempt to deal with this issue.

The committee discussed the need for the FCC to recognize that there are legitimate reasons for restrictive jamming in certain situations.

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

Mr. Victor stated that neither he nor Mr. Elste has seen anything related to this subject in any of the legislation this session. Mr. Berghel stated that he had a piece coming out on this in the next couple months and would send it to the subcommittee members. He would like to discuss this topic again at the next meeting.

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. Elste commented that he thought they had had a great legislative session. He and Mr. Victor have testified on two separate bills and, through their involvement, have gotten the Technological Privacy Subcommittee on the record as a body that is taking these issues seriously.

Mr. Earl stated that a peering bill, cosponsored by Senator Denis and Assemblyman Anderson, looks like it will pass this session. It would require any ISP that provided service to a government entity, to peer within the State of Nevada. During its first introductory session, there was a radical amendment introduced that would call for a study on a peering requirement in the state. That study would be conducted by the IT Advisory Board. The bill was transformed into a bill to modify the statutory provision concerning the establishment of the IT Advisory Board to include this peering study. To Mr. Earl's knowledge, should the study go forward, it will be the first study on peering, including the work done by the FCC. If the bill passes, Mr. Earl will be the staffer from EITS to handle it. This may be a big deal in terms of national attention.

Mr. Berghel asked that Mr. Earl make a presentation on what has transpired on this bill at the next meeting and asked that it be added to the agenda.

Mr. Earl also discussed the recent appellate court decision interpreting a particular provision of the patriot act that essentially said the type of data collection conducted by the NSA was outside the scope, and could not be supported by NSA's reference to the patriot act. This almost makes it certain that the Congress will revisit particular provisions of the patriot act to address the scope of NSA activities. There a couple of statutory provisions in Nevada law that either mimic Patriot Act requirements, or are somewhat contrary to Patriot Act requirements, dealing with data retention for certain types of telecommunications data. Changes to the Patriot Act could indirectly affect some Nevada Statutes that were designed to mirror Patriot Act provisions in state law.

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

The committee agreed to meet on a Friday in early July and will ask Mr. Kandt to coordinate a day and time.

10. Discussion and possible action on future agenda items.

Mr. Berghel asked that the same agenda items be carried over to the next meeting agenda.

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.