TECHNOLOGICAL CRIME ADVISORY BOARD
Technical Privacy Subcommittee

MINUTES OF THE MEETING
March 6, 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. Roll was taken. Mr. Berghel, Mr. Bates, and Mr. Cobb were present in Las Vegas. Mr. Earl, and Mr. Elste were present in Carson City. A quorum was established. Brett Kandt and Laura Tucker from the Attorney General's Office were present in Carson City. Lucas Tucker of from the Attorney General's Office was present in Las Vegas. Mr. Victor joined the meeting in Carson City at 1:35 PM.

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 and thanked them for their participation.

4. Discussion and possible action on approval of January 23, 2015, meeting minutes.

5. Mr. Kandt noted that during the January 23, 2015 meeting, the recorder stopped part-way through the meeting and so the latter portion of the minutes is based on his notes. Upon a motion by Mr. Earl, seconded by Mr. Bates, and carried unanimously, the Subcommittee approved the January 23, 2015, meeting minutes.

6. 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 stated he had been working with Assemblyman Flores, who reached out to Mr. Elste and Mr. Victor to provide assistance in support of the bill which changes NRS 603A, the breach notification statute. Mr. Elste noted that there had been several discussions about the bill and that there is some opposition to it. AB 179 addresses an expansion in the definition of personal information and does a number of things. In its original state, the bill brought in some additional definitions into NRS 603A, such as digital signature, digitized signature, identity theft, and personally identifying information in NRS 205.4617. What Mr. Flores is trying to accomplish with this bill is to eliminate inconsistencies between NRS 205 and NRS 603A regarding personal identifiable information, and to get a definition of personal information which is consistent with federal guidelines, such as the NIST definition. NIST has been putting forth descriptions of personal identifiable information at the federal level for agency guidance that will likely serve as a basis for what ultimately may be federal legislation that is preemptive of the states' breach disclosure laws. Senator Flores has now introduced an amendment that references NRS 205.4617, and replaces the term "personal information" with "personal identifying information" and eliminates the rest of what is in the original Section 1 of AB 179. Section 2 is intact and allows some exclusions such as the last four digits of a credit card number, etc. The current concern is the potential ambiguity in NRS 205.4617 because it was written with the intent of defining "personal identifying information" with regard to the crime of identity theft. It is not necessarily a very crisp definition for implementation of the breach disclosure statute because it covers so many different kinds of identifying information which has created concerns about the potential of implementing it. Mr. Elste distinguished the difference between terms because they are very often used interchangeably:

> Identity – is a descriptive qualifier for an individual. For example: I am a member of the Privacy Subcommittee, or an attorney, etc.
>
> Identifier – personal information that may be part of an authentication mechanism, such as your address or your pet's name.
>
> Identification – the credential we use to authenticate identities.

Mr. Elste explained that the concern today with identity theft is the co-option of credentials. Identifiers can be combined and are commonly used to establish credentials. The risk of compromises becomes much less when more rigorous forms of online identification and authentication are used instead of usernames and passwords. But until that time, there are commonly used identifiers used in creating identification or credentials and if those identifiers are exposed in a breach, individuals must be notified so that they can take measures to protect their identities. The idea behind changing the definition is to be more comprehensive when it comes to defining personally identifiable information in the context of those identifiers that are used for credentialing or authenticating an individual. Organizations that are data collectors and have a breach will be required to notify individuals affected. The challenge is making the definition broad enough to protect citizens and to make sure that the information that needs to be protected is in scope for the breach notification law, and specific enough that it is

implementable from a data collector's perspective. Referencing NRS 205 is a step forward because it's already in the statute and is consistent with the federal language. Federal agencies are using the NIST definition of PII provided in Special Publication 800-122, The Guide to Protecting the Confidentiality of Personally Identifiable Information:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Mr. Elste thought the State should try to strive to something similar – expansive enough in scope to cover the things that are relevant for developing credentials on an individual, and specific enough that it can actually be implemented.

Mr. Kandt speculated that part of the problem may be that a legislator may get an idea to LCB and LCB runs with it without necessarily having the input of subject matter experts in the drafting process. If there is an opportunity to address those issues in the bill with the consent of the sponsor, it is definitely a good idea.

Mr. Victor added that Mr. Flores had reached out to him and Mr. Elste as subject matter experts and was very open-minded. The language may not be correct but Mr. Flores's motivation is correct and he wants to get it right.

The Subcommittee discussed the problem of trying to find a way to provide a slight clarifier on the ambiguity in NRS 205 in the amended language of AB179 to be inserted into NRS 603A. Mr. Kandt stated that although amendments to NRS 205 are not contained in the original bill, that alone would not preclude one from making conforming amendments to 205. It is LCB's call, but making helpful amendments should not be discouraged. Mr. Kandt offered to help with the drafting piece. Mr. Victor said they would need help with the drafting piece because what may be clear to him and Mr. Elste, may be confusing to non-technical people.

Mr. Cobb noted that, for example, a casino video camera may capture images of people in a casino, but it doesn't become PII unless those images are correlated with an individual. He thinks the emphasis should be on the process of matching up, rather than collecting. The PII definition looks like a laundry list of how you collect data and what that data is. It doesn't say anything about matching that data to an individual.

Mr. Earl noted that it is an interesting problem because when you have data that is extracted from an individual, such as a bank account number, it has to be coupled with an individual to become an identifier.

Mr. Cobb posed the scenario of a business accepting a check with a person's name, address, account number and signature – would that then invoke some kind of requirement under the law?

Mr. Elste said that as a data collector, you have an obligation to protect an individual's data. You have an obligation under NRS 603A to provide breach notification in the event of a security breach. Regardless of the definition, the incentive, of course, is not to have a security breach. Increasing the definition of things that have more potential for causing harm to individuals aligns the obligations of the data collector with the harm to the individuals. Currently, the definition is so narrowly defined that if, for example, credentials for online banking are disclosed, there may not be a requirement for a breach disclosure.

Mr. Victor stated that the opposition to the bill includes telecommunication companies CenturyLink and Cox, and the Retail Association of Nevada. The Retail Association of Nevada is more flexible than the telecommunication companies. The lobbyists for both industries are concerned about the language of the bill. The telecommunication companies fear that they will be doing breach notifications on a daily basis. The retailers are concerned about shopping cards.

Mr. Elste said that they had spoken to telecommunications' subject matter expert who is in Washington and is concerned about the implementation of the broad definition and the cost of breach notifications. They are genuinely concerned about the ambiguity in the language and their ability to properly identify and secure the information in scope. Mr. Elste believes there are ways to amend the language to find a middle ground. If they have to, they might want to draw a distinction between those types of PII that require breach notification versus those that are defined in the broader NRS 205 as part of identity theft.

Mr. Elste said they were also approached by a group that represents county clerks, recorders, and treasurers for the state of Nevada. That group has obligations under NRS239(b) to redact personal information from public records on websites. In that NRS they reference 603A as the definition for personal information so if 603A is revised, there may be an explosion in the scope of what will need to be redacted. The relevant statutes are 239B.030, and 239B.050 which references websites and says that personal information shall not be disclosed on websites unless that disclosure is required, with personal information having the meaning ascribed to it in NRS 603A.040.

Mr. Victor asked what 603A says about public documents. Mr. Elste stated that it is not about public documents but about public information. Once something becomes public, like a name and address for example, the information it is no longer covered under the breach disclosure law. However, if that information is used as two components in a credentialing scheme, then it may be included retroactively in the credentialing part of the definition and require a breach disclosure.

Mr. Elste stated that if it the bill is done right, the use of the term "personal information" can be eliminated from the NRS because it's an ambiguous term and not a proper term of art when it comes to privacy and protecting things like PII. It is also an opportunity to

create a much more effective definition of PII in the statute that is more consistent throughout the NRS. He noted that it is good work for the Subcommittee to say they have had these discussions and that they have been asked, because of their subject matter expertise, to participate in and influence the legislative process on a bill like this.

Mr. Kandt asked if the sponsor was asking Mr. Elste and Mr. Victor to come up with some amendments and then submit them as sponsor amendments, or if he wants Mr. Elste and Mr. Victor to submit the amendments themselves. Mr. Elste said that depending on the outcome of a conference call and discussions with the opposition, they will take recommendations for amended language to Assemblyman Flores and he will decide what he wants to do with that language. He has expressed his intent to move forward, in some form, with this bill and is not daunted by opposition to it.

Mr. Berghel stated he looked forward to something purposeful coming out of this. He encouraged the Subcommittee members to think about dark data and think about recommending to the merchants, vendors, and carriers who keep this data to be responsible stewards of it. Perhaps Assemblyman Flores can recommend purge cycles to reduce the amount of such data.

Mr. Elste said that if any Subcommittee members wanted to take a look at the language of the bill and amendments and recommend ways of refining it, to please email him or Mr. Victor. They also invited the other Subcommittee members to provide subject matter expertise by testifying on the bill.

B. BDR 34-147 – Enacts provisions regarding Nevada student data privacy protection.

Mr. Kandt stated that this is the bill that was brought by Assemblyman Kirner regarding student data privacy and protection and it just dropped as Assembly Bill 221. It makes amendments to NRS chapters 385 and 386 which govern activities at the Department of Education.

Mr. Victor said his understanding is that the general motivation for this bill is for entities that are collecting this data to spell out and publish their policies and procedures around the storage and handling of this data. Proponents of the bill want formal procedures to replace a hodge podge of practices surrounding this data.

Mr. Elste noted that in reviewing the bill, it references federal statutes for PII in section two. He suggested that care be taken in publishing data index elements and security practices because it may be detrimental to security. Publishing such information could provide a roadmap for someone with malicious intent by giving them information on what type of data they would find, where they would find it, and what is being done to protect it. There may be an opportunity for additional language that modifies the degree of the amount of information published as opposed to produced and validated by a confidential body. Certain security practices are best kept confidential.

Mr. Berghel urged Mr. Victor to suggest to proponents of this bill that they refer to federal standards for the protection of the data and not get into the minutia of the measures the school district is going to take. There are data protection standards that are widely disseminated and easily found.

C. BDR 44-8 – Enacts requirements and revises provisions for unmanned aerial systems.

Mr. Kandt noted that this BDR has not dropped as a bill yet. The sponsor, Assemblyman Elliot Anderson, asked Mr. Kandt to attend a meeting with law enforcement in which he tried to explain the bill. Mr. Kandt missed the first part of the meeting and so he did not pick up on the entire intent behind the bill, but the bill would create some limitations on the use of drones by law enforcement. Law enforcement had some concerns about the impact on them. Assemblyman Anderson promised to get some proposed language to those attending the meeting but Mr. Kandt has not received anything yet.

Mr. Bates said he has seen the language. In terms of law enforcement, it requires a warrant, with certain narrow exceptions. It seems like a pretty strong bill on privacy issues in general, but it doesn't address some key issues that some other states' bills address. These issues are: 1) record keeping regarding the purpose and the duration, etc. of each flight by law enforcement; 2) the duration of data retention; 3) third parties turning over visual or other information from drone flights to law enforcement, or acting as proxies for law enforcement. Utah has said that law enforcement cannot get that information from private parties without a warrant, and there is nothing like that in Nevada's bill.

He added that the bill also addresses private use of drones. The bill basically says that surveillance in circumstances in which a person has a reasonable expectation of privacy is unlawful. It also has a trespass provision. Mr. Bates said there are some places where, in the name of privacy, the bill may go a bit too far. For example, in a criminal prosecution of an individual who unlawfully conducted surveillance, evidence admitted into court would not be a public record that people attending the trial could see. It would require special permission from the judge. However, Mr. Bates thought that upon his first reading of it, the bill generally seems pretty good.

Mr. Berghel stated that the three omissions regarding law enforcement that Mr. Bates discussed are important to him and he sees them as deal breakers, although the legislature might not see it that way. He asked who on the Subcommittee was working with proponents of this BDR and encouraged whoever has access to the sponsors to convey those concerns regarding the omissions. Mr. Bates will get the language of the BDR to Mr. Kandt who will disseminate it to the Subcommittee members.

Mr. Bates said he reached out to Assemblyman Anderson and one of his aides contacted him regarding hacking so he sent him resources. Then Mr. Bates heard from Assemblyman Anderson asking for copies of everything he had gathered on the subject. Mr. Bates sent him the information with links to several Brookings studies and a copy of a memo he had written.

7. Discussion and possible action on recommendations for creation of a statewide advisory board on technical and digital privacy.

Mr. Kandt said that at this point in time—in the middle of the legislative session and with the new administration getting a handle on the full spectrum of issues at the Attorney General's Office—he thinks that General Laxalt would like to work through this group, and get its recommendations, under the existing framework. It is something that can be revisited at a later time, but for the time being, General Laxalt wants to hear from the Subcommittee working in its current composition.

Mr. Elste commented that with the bills just discussed, and with active engagement from this Subcommittee, the discussion post-legislative session becomes a much more interesting one. He suggests going forth and focusing on what is on the table already, and revisit this issue in the summer.

8. 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.

Mr. Kandt stated this proposal is certainly something that can be brought up with the Attorney General at a Subcommittee meeting, or a future meeting of the Tech Crime Advisory Board, but there is no movement on it right now. The two members of the Board that are legislators did not submit any proposals along these lines. There are several proposals to amend the Constitution in one way or another but this isn't among them.

Mr. Victor said that, going along with the logic of Mr. Elste regarding the structure of the Subcommittee, these are the types of items they can talk about in the interim. He thinks if the Subcommittee keeps doing all the good work they have been doing on the bill drafts, they will have a lot of momentum coming out of the legislative session.

Mr. Elste stated that the topic bears continuing discussion so they will be ready when the opportunity comes up to revisit the issue with the Attorney General, or TCAB, or whomever. It is still the Subcommittee's position that there should be an amendment to the Constitution as discussed and agreed upon during the Subcommittee's previous recommendations It can sit dormant until an opportunity presents itself for further discussion.

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

Mr. Kandt reported that this item is in a similar status as agenda item 7(A). Neither of TCAB's board members who are legislators chose to take it up and so it is left for future discussion.

9. 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.

This topic was covered during the discussion of agenda item 5(A). Mr. Berghel asked if there were any further comments.

Mr. Elste asked if, during his testimony at the legislature, he could reference the discussions that the Subcommittee has had and note that those discussions are on the public record and that this topic has risen to the Subcommittee's attention. He thought referencing these discussions would be very valuable and would put the existence of the Technical Privacy Subcommittee on the record. The Subcommittee had no objections to Mr. Elste' proposal.

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

Mr. Berghel asked Mr. Bates if there was an update on this topic. Mr. Bates stated he had not heard of any additional litigation, or of other states dealing with it. He does think that coming up with an approach to restrict these systems is a reasonably high priority for future discussions for the next legislative session. There is the issue of law enforcement use of it but also, equally significant, is the issue of private use when the records are turned over to law enforcement upon request.

Mr. Berghel asked if Arkansas had withdrawn its Automatic License Plate Reader proposal. Mr. Bates stated he believed that Arkansas was challenged and the case was dismissed on sovereign immunity grounds so as far as he knows, Arkansas law is still in place and there is an appeal of the dismissal underway. Utah has backed away from legislation. Mr. Bates said he believed that there was a New England state that also has a restriction and at least one other state that has its Attorney General's guidelines on it. Mr. Berghel agreed that this is an important issue and recommended the Subcommittee discuss it at the next meeting.

Mr. Elste noted that license plate reading in this context is not about identifying a plate but about identifying a person so it is almost an issue of PII, such as discussed earlier. It may set the stage for these kinds of derivative identifiers to be brought up.

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

The Subcommittee discussed whether there was a generally agreed upon definition of the word "metadata?" Mr. Elste stated that his understanding is that metadata refers to

non-content data. For example, during a cell phone communication, the content data is the voice communication. The metadata would be the cell phone carrier, the phone numbers, the time the communication took place, the location, etc. Ostensibly the argument is that metadata is not the communication, therefore it is not surveillance or otherwise infringing on someone's right to privacy. It is ambiguous right now whether metadata is or is not protected.

Mr. Berghel stated he thought the reason they had proposed discussing this is that whether you consider metadata exclusive of the object data or not, it is very valuable information which betrays a lot about the people over which it is collected. The spirit of this question is whether we should we be more a little more aggressive in requiring standards in regards to its collection, dissemination and use.

Mr. Elste agreed and noted that metadata is a construct that most people do not have a clear understanding of but it is almost as valuable as, and sometimes more valuable, than the actual communication. Law enforcement may find that where two suspects have a conversation is more important to an investigation than the conversation itself. There should be suitable processes to access to the data and protections for individuals not under investigation or other forms of legal surveillance from wholesale collection of that metadata. Metadata can reveal very detailed information and patterns of behavior about people which can create a digital fingerprint to identify a person. It is a class of data that needs to be looked at from a privacy perspective.

Mr. Berghel asked if there was room for this topic in Mr. Elste's discussion with Assemblyman Flores regarding breach disclosures, etc. Mr. Elste stated that he didn't think they should pile on the PI bill with the metadata question, but it is part of a broader construct around how data is treated and how to establish legal rules that recognize the value of the data and how it relates to individuals' privacy. Failure to do that will set us up for a very, very long period of time trying to unravel the capabilities of systems in place to take advantage of that data.

Mr. Berghel acknowledged that they can only fight so many battles at once but doesn't think there is any logical reason to separate this issue from the one already being worked on. He recommended the Subcommittee continue to discuss this issue and see if they can come up with something purposeful that would help the citizens of the state.

D. Proposed telematics black box legislation.

Mr. Berghel said that, so far as he knows, not a lot has changed since the Subcommittee last discussed this topic. The motivation for using the black box came from the insurance industry. Opposition was so strong in California, that the bill about it was withdrawn. Mr. Berghel thinks this is an important issue, but it does not seem to be getting a lot of traction. Mr. Berghel stated the Subcommittee would continue to look at this.

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. Bates said he did not think this should be one of the Subcommittee's higher priorities. The FAA requires the test site to have privacy policy but, so far as he knows, does not approve it. The policy in place now could use some improvement, but working on it is probably not the best use of the Subcommittee's time given its other priorities.

Mr. Elste suggested the Subcommittee make an offer to provide guidance and assist the Test Site in revising their policy when they believe it is time to do so. In that way, the Test Site will have an avenue towards improvement and accessing some expertise. Mr. Berghel said he would contact Mr. Cunningham from the Test Site to make that offer.

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

Mr. Berghel noted that his article on Noirware is in the current issue of *IEEE Computer,* and is essentially about the information Mr. Berghel provided to the Subcommittee at the last meeting. He said that it is an example of technology absurdism that we launch these technologies without an appropriate understanding of what the negative externalities are. There is no consideration given to the blocking of RFs which could result in a lot of damage. There is nothing you can do legally to defend yourself from a RF transponder surveilling you or capturing privileged communications. Mr. Berghel thinks that has to change at a federal level. Mr. Berhgel said he will continue to update the Subcommittee about the issue.

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

Mr. Victor stated that the controls over mobile devices have an over-arching goal primarily focused on stopping the theft of mobile phones and concern for public safety over the possibility of physical harm to victims during a robbery. The motivation for many of these crimes can be the high premium paid these phones command on the black market, especially overseas. The State of California has implemented a law, mandating a kill switch on many mobile phones. The law says that a factory wipe, or factory reset, cannot be used as a mechanism to defeat the kill switch. In most cases, that means a central service, such as the carrier or another third party must enable a remote kill of the phone.

There are a lot of exceptions which, Mr. Victor noted, have not been discussed in the press. For example, the manufacturer can make the claim that the phone's design does not allow for the retroactive application of the kill switch which may cover a significant percentage of devices. The Subcommittee discussed how this may mean

grandfathering in not only phones that have already been sold, but also phones that continue to be manufactured without that capability. There is also a huge market for refurbished phones which would be exempt.

For phones designed from scratch, the law says that a third-party carrier or technology company must be able to send a kill switch to disable the phone and delete the data remotely. However, many users are much more concerned about the data on their phones then about the phone itself. They don't want other people to have their data, but they want to be able to preserve it for themselves. Kill switches disrupt data integrity and data availability which are two of the pillars of information security.

Many of the kill switches are tied to GPS. A lot of consumers and businesses that want to protect employees have trouble with the constant tracking with GPS and want to disable it. Since some of the kill features are tracking with GPS, it can prove problematic.

Another feature of the California law says that end users can disable the kill feature if they wish.

Mr. Victor posed the question that with so many exceptions, how much protection does this law really offer? Based on his experience, encryption is what is really needed – not a kill switch.

He noted that there is a company called Absolute Software that has a complete suite of different types of options for remote kill, remote wipe, and remote capture. This company has worked with some of the major phone manufacturers to make these features available so it seems that the market is responding in a variety of ways to what the demand is related to the general topic.

Another issue that isn't really covered in the law are the dramatic changes going on in the mobile phone industry. The traditional model is that a consumer walks into a carrier's store and buys the phones directly from the carrier. The kill switch can work well with that model because the carrier has direct control of selling the phone and putting their branded firmware on it. But the market is shifting to a new model where a consumer or business buys a phone and owns it outright. The phone is not tied to a specific carrier. The consumer activates the phone with the carrier they wish to use and then consumer has his own software on it. Blu and Vizio are an examples of this kind of company, and they are quickly growing. The California law applies to phones bought in California. Many phones are sold on the internet from companies that may be outside of United States and so the jurisdiction of state laws may not be applicable. The Blackphone, for example, is a privacy-oriented smartphone with its own operating system run out of Switzerland because Switzerland has very strict privacy laws. Other countries may not be amenable to some sort of reciprocation because they do not want government control on these types of devices.

Another class of phones are not even on the cell phone network. They look like cell phones but aren't. Examples of these companies are Republic Wireless and Theater

Pop that make the calls over wireless devices. The ability for the State of Nevada to control the phones that are sold to Nevadans is declining rapidly.

Kill switches are a mandated back door to the phone and back doors can be used by for both good and malicious activities. The kill switch also requires power and a signal. So if someone wants to steal a phone, he will need to get power out of it or make sure the signal doesn't work, which is quite easy to do with signal-blocking bags available on the internet. Any kind of system like this has a potential work-around.

There are a lot of issues with any kind of kill switch. The good news is that there are a lot of startups and companies coming up with different varieties of solutions to the kind of kill switch that consumers want.

Mr. Victor said he thinks we may see this issue fade. The theft of phones may be a result of the early stages of the mobile phone industry where you have two dominant providers: Apple with iPhone and Samsung with their Galaxy series. As the market becomes more diffused, demand for certain phones on the black market will also diffuse. The rate of change of cell phones is also dramatically increasing. There is a Chinese company that manufactures fresh products and versions every six months. The rapid change will make it difficult for a thief to know what model to target for the black market.

Mr. Berghel stated that to try to pass legislation with technologies that are not well thought through in terms of the balance between the positive and negative externalities, is ultimately not very useful. He would not recommend legislation because California already has a law and whatever California requires will affect Nevada. It is something the Subcommittee should think long and hard about before getting involved.

Mr. Kandt noted that this legislation had been submitted by the previous Attorney General. He recommended that Attorney General Laxalt withdraw the BDR for many of the reasons stated by Mr. Victor and Mr. Berghel. It is dangerous to statutorily mandate technology solutions.

Mr. Elste said that on a very high level, it is kind of Orwellian to have a mandated kill switch on devices. He doesn't really buy the fundamental premise of the law that it protects consumers. If that were true, there would be kill switches on automobiles and guns. The notion of a kill switch is not fundamentally an effective deterrent to crime. The other parts of this bill include a rather broad loophole for law enforcement and state and local agencies, which could, without a court order, based on exigent circumstances, activate kill switches. Smart phones are also defined rather narrowly in the legislation, when other devices can also be used for communication. Nothing in the legislation talks about wiping the data off the device. It only talks about disabling a device, which may not be in the interest of the consumer.

10. 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.

There were no further comments by the Subcommittee.

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

Mr. Kandt said he would check availability of the rooms for late April or early May. The meeting was subsequently set for May 8, 2015, at 1:00 p.m.

12. Discussion and possible action on future agenda items.

Mr. Kandt said he would keep track of legislation and bring anything that might be of interest or relevance to Subcommittee. He asked the Subcommittee members to email him if they have anything they would like discussed.

13. 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.

14. Adjournment.

The meeting was adjourned.