TECHNOLOGICAL CRIME ADVISORY BOARD

MINUTES OF THE MEETING

June 5, 2014 at 2:00 pm

Legislative Counsel Bureau
401 South Carson Street
Carson City, NV 89701

Video-conferenced to:

Grant Sawyer Building
555 East Washington Avenue, Room 4412
Las Vegas, NV 89101

AGENDA

The Technological Crime Advisory Board was called to order at 2:00 pm on Thursday, June 5, 2014.

Advisory Board Members Present in Las Vegas:
Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
James Owens, Deputy Chief, LVMPD, meeting designee for Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Professor Hal Berghel, University of Nevada, Las Vegas

Advisory Board Members Present in Carson City:
Tray Abney, Reno/Sparks Chamber of Commerce
Kyle Burns, Resident Agent in Charge, Homeland Security Investigations
Nevada Senator Aaron Ford (via phone)

Advisory Board Members Absent:
Assemblyman Paul Anderson
Dennis Cobb, Co-Director of the UNLV Identity Theft and Financial Fraud Research & Operations Center.

Staff Members Present:
Brett Kandt, Advisory Board Executive Director

Others Present:
Edwin F. Mansoori, Palentine Technology Group
Allison Hodges, Palentine Technology Group
Carolyn Schrader, CEO of Cyber Security Group
Barry Smith, Nevada Press Association
Brian Spellacy, Special Agent in Charge, U.S. Secret Service

Mr. Kandt: William Uffelman is retiring and no longer on the Board. The U.S. Secret Service Special Agent in Charge Richard Shields has retired and the new Special Agent in Charge who I believe is present down south. Brian Spellacy is with us today. Brian has agreed to serve on the Board. Brian, did you receive notice of your appointment from the Governor's office yet?

Mr. Spellacy:
I have not.

Mr. Kandt:
For purposes of a quorum, I would recommend that we not include Brian today among our quorum for purposes of taking action. That's it, we have a quorum.

Agenda Item 1 – Call to Order, Verification of Quorum.

The Technological Crime Advisory Board was called to order by Chair Masto and a roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Public Comment.

General Masto asked if any member of the public would like to address the Advisory Board during this public comment time. It appears there is no one so we will move on.

Agenda Item 3 – Discussion and possible action on approval of March 6, 2014, meeting minutes.

Mr. Kandt:
There are two minor corrections on the first page. Member present in Carson City: Assemblyman Anderson was actually present in Las Vegas. With regard to Mr. Abney, his name is misspelled and he is not represented properly. He is actually with the Chamber of Commerce. Any approval of the minutes, I will ask that those revisions be included. (sp. Tray Abney)

General Masto: Any other edits, changes or motions?

Mr. Burns: I make a motion to approve the Minutes for March 6, 2014. Mr. Owens: Second.

General Masto:
Any further discussion? Hearing none, all those in favor of approving the Minutes from March 6, 2014 meeting signify by saying "I". Those opposed "nay". The Minutes have been unanimously approved.

Agenda Item 4 – Presentation on Electronic Warrant Interchange (EWI) from Edwin F. Mansoori, Palatine Technology Group.

General Masto:
Thank you, Mr. Mansoori, welcome. I understand you have with you Allison Hodges who will be assisting you with the presentation. We appreciate you being here today.

Mr. Mansoori:
Thanks for having us here today. We have prepared a demonstration for you of about 45 minutes and a short presentation and video. Some of the videos are dated videos because this product was originally started in Georgia in 1998. It was originally approved by Georgia's Supreme Court as a test project to allow law enforcement to obtain arrest warrants electronically from the magistrate. It was so successful that the following year they decided to do the search warrant and passed it as a law in Georgia. Now they can do arrests and search and blood search warrants electronically via this system. (PowerPoint presentation).

Ms. Hodges:
I'd like to point out that the videos are a little dated because this product was rolled out in 1998. It has since been updated continually with added modules and technological advances. The Electronic Warrant Interchange (EWI) is a patented middle ware product that provides a central platform to generate and track warrants. It provides seamless integration with all RMS and CMS platforms. It is a cost reduction tool reducing the cost of a warrant from the manual approximately $285 to an electronic one that only about $38. You can see it will pay for itself very quickly. It's currently used in over 70 agencies and over a million warrants have been issued by EWI. It has built in logic that ensures accuracy of data and prevents critical omission. It generates arrest and search warrants from anywhere via a secure link to the internet. It's compatible with Windows or Android tablets and it has legally binding forensic-grade electronic signature with date and time stamp. It's available for single county, district or statewide implementation. It's easily configured to multi-level approval processes. We duplicate your agency's forms and it supports multi-language documents. It's name compliant for sharing data. Pictures and video files can be attached to cases and reviewed be all concerned parties. Conference calls can be recorded and stored as evidence of legitimacy of the warrant and evidence for discovery. (Another slightly dated video).

Mr. Mansoori:
This software uses a LED based technology to display the information in a browser. It does not have a Windows interface. However, it uses a secure link to your internal server. When we talked to different agencies about the system, we tell them it's a web technology that you will go to get the warrant. This is not a web base that everybody can go to and get information. This is specifically designed for law enforcement to access using 128 bit encryption to access the site and get their warrants. To access the system, they would have a unique user ID and password. It's basically one page where they would enter all information about the parties. I have entered a case already here in the interest of saving time.

General Masto:
For the members up north, can you see the screen Mr. Mansoori is working from?

Mr. Kandt:
Actually, we can't. We were able to watch the videos but we aren't able to see the screen. We do have the supporting material. Now, we can. Thank you.

Mr. Mansoori:
This is the screen that law enforcement uses to enter their information. On each section, you have different parties where you can enter the information. All the fields that are labeled with direct ___ , those are mandatory fields – those are the fields that absolutely have to have an answer to it before the system would allow them to save the information and have a valid, legal warrant. If any of this information is missing, the information cannot be saved. The system is capable of generating the warrant in multiple languages so when the paperwork is generated, you can have it in a different language than English. Once the information is entered for the accused and victim, you can have a different type of victim, you can have a business victim, you can have the state as a victim, and also you can have an infinite number of accused, victims, and witnesses in the case. There is no limit as far as how many parties you can in a case.

Once the information is entered, they click on save and the way we have designed this, it has an interview function that it tells the officer that this is what you have done so far and this is what you will do next. There is no confusion as what button has to be clicked next or anything like that. Once the information is saved, they enter the offence information. To add an offence, the way we have done this on each state's statute, you have major category of crime and under that, you have different offences. If I need to add another offence, I would select the keyword and under the keyword, I would select the offence of burglary. I highlight burglary and it gives me all the offences that are related to burglary under this state statute. I select burglary and it gives the officer a boilerplate description of that offence. They usually get this from the column charge book and the DA's offices have all these texts already assigned to each offense. Basically, what we do after the officer enters this information, text will show up in the offence description and then you can click on get variable and it gives a blank area that they can enter the felony name. As you see on the left-hand side, all the possible choices are there. If it's not there, they can type in whatever they like to put in there and click on replace variable. Also, it has a built-in spell checker which is just like your regular spell checker that you are used to using. If there is a lengthy probable cause, they can enter it in the probable cause section with the option of clicking on print on warrant so the judge can see it and be printed on the body of the warrant or they can just leave it for the judge to see to make a determination. I have entered the offence location on the first offense and I click on the link to give the previous location if it has happened at the same location, I click on select, and it copies the offense time and date in my next offense. Click save and if you have another offense for this accused, no, then I am ready to contact the judge.

All the forms we generate in here, basically, are coming from your police department and your agencies. We don't any of our own forms. Once we complete this, you will have your own forms so it will be a shorter learning curve to learn the new system. Everything is generated in PDF format. I'm using this air card right now, that's how I'm connecting to our office in LA; I'm not using your internet. You can be anywhere and issue the warrant or obtain a warrant from a judge using the air card. This is actually the document that would be generated. When they are ready to contact the judge, they click on video and we have our own built in video system that actually is a soft phone which is new concept, it's called Voiceover IP that uses your network to communicate for video and audio. It's something you typically have on a new phone system, like Cisco, you have voiceover IP phone. It's very reliable and very robust. I have my computer set up at the

office to answer this call as if we were calling the judge but his is my office in LA. As you see, the video is clear; there is no pixilation even with the air card. The judge has the option of recording the conversation with the officer. In some big cases, they like to record the conversation; they have that option. What it does, it is saved on a server on the judge's machine and it's converted to an AVI file and it's part of the case as long as the case exists on your server. You can always go to that file and see what has happened. This is basically what the officer does with the arrest warrant.

To do a search warrant, the screen is a little different. We can different types of search warrants, for a person, location and also we have a blood search warrant which is becoming popular these days for DUI cases. If the individual refuses a Breathalyzer test, they can do the blood search warrant. To start the search warrant, they can select either the search warrants for the person or location. Cash, drugs, guns – if there is a typo, it underlines it in red. They can put the probable cause in here. The location of the search warrant is entered on the street field where they need to conduct the search. Also, in the production version, we check the location that is entered and we check it Yahoo Google Maps and make sure that address is a valid address. Also, in here you would be able to check the Google Map and see a map of the location and if there is any picture available. You can actually get the street view of the location for the search. They can ask for no knock in some states. That's pretty much all the officer has to enter into the system to get a warrant. If I save this at this point, I can look at the search warrant document. It only takes a few minutes to enter all the information. In comparison to the old fashioned way, warrants are generated within 10 minutes. Typical manual warrant that is generated without EWI takes up to a couple of hours without an electronic system.

There is another module for the judges which is called Judge Module. They have the officer on the side of the screen on the video and they can have a conversation with the officer. They would ask for the case number, and the judge would enter it and it would show up here. It displays all the information that the officer entered on his computer in this format. The judge has total control of the information. They can look at what the officer has entered on his end and he can look at the screen the information was entered on. There is a dashboard where they can look at all the case information based on the information that has been provided in the system. At this point, all the judge has to do is set the bond; each offense can be set for a different bond. Now the judge would ask the officer to sign on the screen. The judge has to click on the review button which indicates the case has been reviewed by the judge. The officer would sign and now the judge can sign. This is your finished product. It time and date stamps the signature, the name of the office who applied for warrant and also information for the judge.

General Masto:
Is this product being utilized anywhere in Nevada?

Mr. Mansoori:
No, not in Nevada.

General Masto:
Does anyone know if we are doing any type of electronic warrants?

Mr. Owens:
We have tablets that we use. We use telephonic warrants.

General Masto:
Brett, I haven't looked at the laws – do the laws allow us to do an electronic warrant?

Mr. Kandt:
That's one proposal that I had brought to the Board and you referred it to the Technical Privacy Subcommittee. We will be discussing it later on the agenda. I am of the opinion that our statute which is NRS 179.045 doesn't expressly provide for or even contemplate the application of or issuance of warrants via electronic transmission. I would recommend that we seek an amendment to statute in the next session to expressly provide that authorization.
General Masto:
Thank you. Is your product utilized in how many states and which areas.

Mr. Monsoori:
Currently, it's only in Georgia. We have sold it to one county in Texas and we are working on selling the product to the other states.

General Masto:
Say a locale, just a county, wants to implement it; the costs associated with it would include, besides the application software program, the hardware that would be necessary for it? Are we talking a lot of hardware or is it compatible with their existing hardware?

Mr. Monsoori:
You can use with newer existing hardware, however, the judges in some larger counties, like the City of Atlanta, we have judges that have laptops that they take home at night. Officers have access to a judge 24 hours a day, 7 days a week. With the new advances in technology, you can have a tablet that the judges can have with them and issue the warrants from anywhere as long as they have an air card.

General Masto:
Questions or comments?

Mr. Owens:
I know some of our personnel are working with Brett on this. I don't know if it is fixing a problem where we don't have a problem. I'm not sure but the ability for us to do telephonic warrants has been critical.

General Masto:
I suspect the reason why we would be looking at this as well particularly for our rural areas where there may be a distance between law enforcement and the judges and trying to get warrants they need. Any other comments?

Mr. Abney:

I'm looking at the documentation here and it says that this is in use by over 70 agencies. Does that mean all 70 of those are in the State of Georgia? Various agencies and counties?

Mr. Mansoori:
Correct. Most major counties in Georgia are using this system now. In the large population centers, they use the system.

General Masto:
Any more questions or comments? Thank you very much – very impressive technology, cutting edge, we really appreciate you being here today. Let's move on to our next agenda item.

Agenda Item 5 – Presentation on cyber threats to small and midsize businesses from Carolyn Schrader, CEO of Cyber Security Group, Inc.

Ms. Schrader:
What I wanted to do today is share some information about cyber security for the small, midsize market space and give you some information. First, I'd like to talk about the threats, what the impacts can be, a little bit about what hacking is because we often make assumptions based on what we hear in media, what the cost is and then talk about some of the opportunities of what we can do going forward.

In 2013, every major corporation was hacked. A statistic that came out last week said that on an average, 135 instances per business per year. That's a couple every week that are being hacked. They also have identified at least fifty percent of small mid-size businesses are being hacked. The numbers are hard to track because there is not a lot of very good reporting yet. We do know that the cyber criminals no longer care what size of business or what kind of data you have. There is such an opportunity out there to re-sell the stolen information. It's a borderless crime that brings all sorts of different dimensions to it than other types of crime. We know a number of countries that are very powerful in the cyber-criminal world with gangs and a lot of focus and attention sponsored by both independent efforts as well as state efforts. One of the interesting ones that has been added to the list was last week the former Secretary of Defense identified France as a country that is very big in industrial espionage. We see this everywhere, not just a couple of countries that we normally think of.

One of the biggest breaches prior to EBay of a week or so ago, was the Target data breach where 40 million customers' records were impacted. What is not as well-known is the entry originally started with a mid-size business. Fasio Mechanical is a company based in Pennsylvania and was doing HVAC – heating and air conditioning work for Target stores. Someone was able to hack into their system, steal a number of things, including credentials that allowed them then to penetrate Target. Target, of course, had some flaws in their security which allowed it to happen. Initially, it came through a mid-size business.

I would like to talk about the major threats that we see to the small, mid-size market. A little bit different focus than what we see with the larger businesses. Malware is very sophisticated nowadays. It's very targeted, it's very secretive and it's using the business' network to distribute for even more access of information. Last year, the numbers were staggering. 80

million new malware programs were identified in the year. The first report that we've seen for this year, for Q1, was 15 million so certainly on track and will probably increase as we progress through this year. These are variations on a theme, these are new approaches, new malware, all of which are out there in the wild.

The second threat is this new, growing world of internet of things. Things can be very small like a baby monitor or it can be huge such as entire building's system control system. If it has an ability to be programmable, it often has the ability to be connected to the internet and therefore, it can get to smarter devices. You know have so many entry points – you've got such an increased risk and unfortunately, most of these devices do not have security in them. Number one because that's an extra cost to the manufacturer to put into it; there has not been the customer demand for it; and the technology certainly exists but it has not yet been implemented to secure so many of these devices.

The small business world is now being impacted greatly by bring you own device (BYOD). We see this in large corporations. They've had it for some time now. They let employees bring their own Apple, their own Android, whatever device, tablet, smart phone. The challenge for a small business is that they intermingle their personal data with their business data. You have a lot less control as a business owner of your data and the individuals usually don't put security measures in place. Now you have a lot of data available on a lot of devices by a lot of different people and unfortunately, these are frequently stolen or lost. How many times do we hear stories of someone losing their phone in a bar or leaving it in a taxi cab or wherever it might be? We are now seeing in many major cities that the stolen smart phones is the fastest growing street crime out there. They want not only the phone that they can resell; they want access to that data.

People don't know that there's this incredibly huge black market for data. We hear that it's being stolen – so what – who uses it, where does it go, what happens to it? There's massive money out there in this illegal hacking world. The organizations are incredibly sophisticated. They have hierarchies; they have job functions; they recruit for specific activities and skill sets; they're very creative marketers just like an ethical, reputable company. This picture here happens to be selling a doctor email list. As you can see at the bottom, you can even buy it with PayPal and by the way, there's a discount this month for it. They use a lot of tactics we are familiar with reputable businesses.

The fifth threat we are seeing in the small, mid-size space is increased malware being attached to a website. They will go after a very reputable website, take it over as a distribution source. Then, any visitor that comes to site becomes an unsuspecting conduit for this malware. Without knowing if you've gone to a reputable site, you are now infected if your antivirus doesn't catch it. It will then permeate through other connections that you make - all to steal more data.

Hacking we know so much about is stealing credit card information. We know a little bit, we hear in the media about medical information but sometimes we forget about or don't realize all the other kinds of hacking that goes on and how we can prevent it. If we prevent it, what we can do about it going forward.

Data types can be anything from passwords; they'll go after trade secrets; they will go after research; they will go after blueprints; client lists; financial projections; anything that another business can utilize. Anybody that has information that makes their business successful – chances are somebody wants that if they can get to it. They might be using it to sell to a competitor and that competitor might be in China. One case is a company that sells of all things, hair extensions. The competitor in China tried to take a San Francisco company offline because he wanted the entire global market space for hair extensions. Very damaging to that small, local business. It could be a local competitor that it's being sold to. They want to pirate a product – why do your own research if you can pirate the blueprints or the plans or the patents for something and take it from there. Again, being a global business of hacking and selling all this information, it's much easier in many of these countries is just steal from America and certainly other places, as well. Certainly, the issue of hacking in to get access to a larger business or organization is very common unfortunately.

The impacts to Nevada residents is certainly on an individual basis. The stolen personal information, losing your bank account information, identity theft, whatever it might be. Then also, you have your economic impact to the state itself, to the businesses. They identified that 60 percent of small businesses after a serious attack, go out of business so we have lost those small businesses to our economy.

Another thing that we are starting to hear about is the detraction for new business moving in. Big focus now is on supplier chain security. If we try to encourage large businesses to use local suppliers, they want to know that those local suppliers are secure, that they do have the measures in place. Obviously, there's an incredible cost with prosecution for any cyber-crime.

Talking about cost of recovery, from a business perspective, Ponaman Institute identified, for 2013, it is upwards of $200 to $246 dollars per stolen record. You can imagine how quickly that escalates if you have lost your credit card information, if you've lost your patient information. Just astronomical costs can be associated to recover. The Target breach, for example, they are still debating how much and they think it's going to top a billion dollars. The reason these costs are so high is you've got to certainly, as a business, pay for your legal representation. You have to have counsel to get you through the issues of recovery. You may be subject to lawsuits, either from your customers or some of the states are starting to sue businesses that have not adhered to the notification laws. Almost every state has a notification law but they are all different. If you have customers in five states as a business and you've had an attack, you now must notify your customers in five states using five different approaches potentially. You might, if you've lost customer data, you may have to pay for ongoing credit monitoring services. Of course, you have to go back and fix whatever that initial problem was and you darn well better go in and assess what other security flaws you have as well so you don't have a problem again.

I have a couple of slides from my associates over at UNR. They have recently established a cyber security center. One of the things that is unique about what they are bringing to Reno and Nevada as they build this center, they are taking an interdisciplinary approach to it. They want to look at it beyond it being technological. They realize that this is a human issue. This is a legal issue and how can they put these pieces and parts together. Their mission is that they have identified it so far is to perform research, they want to do some education, what they excel at, they are going to offer next year, a graduate certification program in cyber security

and they want to very aggressively interface with the work force, the businesses in Nevada and provide trained resources.

A quick overview of some of the other states and what they've been doing:

California has recently posted a cyber security site exclusively for small businesses. Attorney General Harris has put this up and has some good resource information.

A number of states have through their AG office, tips and links similar to what Nevada has provided. There's not an awful lot when one thinks about the size of this crime and the broad penetration and the impacts of it. As we all move forward and learn more about it and worry about how we handle it, opportunity for certainly more actions. I've identified a handful of actions – some of which are probably already in process – may need additional support, may warrant some additional thinking as we move forward.

The prosecution at the local level – even though this is a borderless crime, we do find that often the computer terminals, for example, the hardware may sit in the United States. They may be managed out of the Ukraine or out of China but the actual hardware may be here. The recent warrants that were handed out for the Chinese hackers that were identified actually came out of Pittsburgh Federal Jury. So there is local action in different reasons that different states get involved with it. Certainly, an opportunity for more sharing with local law enforcement on how to do investigations. If an attack happens in Elko or in Henderson, do those law enforcement agencies know how to move forward? We certainly know the businesses are naïve because they haven't done this a lot yet. They don't know how to manage the evidence and to make sure that it's a legitimate and effective investigation. One of the things we're hearing and starting to see at the federal level coming down a bit more even for the small businesses is how we facilitate information between law enforcement and cyber security professionals. Inforgard, for example, just in the last 45 days or so, a lot more information has been shared and communicated down. They feel that one of the biggest advantages is we identify trends amongst the criminals is the fact that there is information sharing through industry as well as through geography. There certainly needs to be a stronger awareness among businesses. They are coming out of a recession, they've worried about staying alive, making a profit, expand their market, opportunity to help them understand what the risks are but how they can protect themselves because there are many secure businesses out there. They can do many actions to take care and reduce that risk. Certainly, cyber insurance is starting to play a stronger role.

My last action step for consideration is we will have to have some level, as a society, of requirements just as we've had to do for many other bad behaviors. Sometimes you have to do the carrot and the stick that we can talk good things and help businesses be better, make sure they have avenues. Can we incent them, perhaps to do better behavior, can we also realize that we are going to have to give them some punitives to make them behave. Not everybody will do the good thing by themselves, unfortunately.

Those are my comments. Is there anything I can answer for you?

General Masto:

Miss Schrader, thank you so much. Very informative. My first question is what does your company do?

Ms. Schrader:
I am a startup company focusing on small mid-size businesses helping them prepare themselves. Everything from penetration tests to doing consulting on what kind of training awareness they can do, policies, procedures, etc. We focus on consulting that market space.

General Masto:
Thank you. Questions or comments from Board Members?

Mr. Berghel:
Just a point of administrative trivia for you, nothing to detract from your presentation, but UNLV created a cyber security program at the bachelors, masters and PhD level in 2005 and implemented it that year. Reno, to their credit, has a program but it wasn't the first one in the state and they were very lucky as things played out, to be able to displace us in that role. The reason I know that is you just happened to make a presentation to a board that consists of the person that created the program at UNLV.

Ms. Schrader:
Excellent – the more programs we have, the better we are.

General Masto:
Any other comments or questions?

Ms. Schrader, one other thing that I would point out from the experience we have in the AG's office and you've identified the what and why individuals engage in this type of this activity. On page 16, the other thing that we are seeing and I'm sure you're aware of it is this issue of breaching or hacking into small businesses data base and gathering their information and then locking the business out and then blackmailing them or extorting them to get their documents and data back. Unfortunately, that is occurring as well. I know it's happening with a lot of the small businesses as well.

Ms. Schroeder:
The sad thing is they filed against the people of crypto lock that have been real common recently but one of the commentators said they'll be back in business in two weeks. Unfortunately, as soon as you lock down, we unfortunately tend to have others. It will be a problem we have to continue to address.

General Masto:
Thank you for everything you do. We really appreciate the presentation today. Absolutely eye opening and definitely on our radar to address this issue of cyber security for our small and mid-size businesses.

Agenda Item 6 – Reports regarding Task Force and Board member agency activities. (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.

General Masto:
I know we don't have some of our board members with us officially so is there any member right now who is a voting member that has an update for us?

Mr. Berghel:
One of the research projects that I'm working on right now has to do with predictive capacities for future money laundering. I don't know if that has interest in the Board but I'll have that work completed within the next month and what I'm focusing on is where money laundering has to go to circumvent existing regulations and law enforcement prosecutions.

General Masto:
From my office's perspective, we'd be very interested. We are actually, part of my bill package is looking at our money laundering statutes to address those and looking at how we address this issue particularly in the State of Nevada giving investigators but more importantly, prosecutors more tools that they need. We'll reach out to you through Brett and make sure we're communicating and understanding the research that you've done would be very informative for us.

General Masto:
Any other comments from Board members regarding Task Force work that they may be conducting at this time.

Mr. Burns:
It's more of a job well done. HSI is up in our area, we are a major part of the Northern Nevada Internet Crimes Against Children Task Force run through the Washoe County Sheriffs' Office and we had a conviction last month, a Carson City resident got 19 years on federal child pornography charges. He was a substitute teacher in Carson and Lyon County and we worked hand in hand with our local partners and it was one of the stiffest sentences that they've handed out. This gentleman was very egregious in his activities. He had pinhole cameras in his own house videotaping family members and he shared it with people in 15 countries around the world. This is what the DA said would be the most egregious case of child pornography production she has ever seen. It was with the help of our state and local partners that we were able to put that bad guy away for the next 19 years.

General Masto:
That is a job well done – kudos from all of us, that's fantastic work. Thank you very much.

Agenda Item 7 – Report from Executive Director. (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:

Thank you, Madame Chair. I'll keep it short but following up on Ms. Schrader's presentation and the discussion about improving the capacity or building the capacity at our state and local level to investigate and prosecute tech crimes through collaboration with our federal partners leveraging their resources. We are doing that but we continue to try to explore ways to further leverage those resources and build up that capacity on the state and local level. Everything, obviously from sending our personnel to NCFI for training, in fact, one of our prosecutors in the Attorney General's Office, Sam Kern, just returned from that training last month. Then, on the other level, bringing the training to us and we are working with our local partners at the Secret Service, they are going to provide some training at the prosecutor's conference in September. There will be about 100 state and local prosecutors there and the Secret Service is going to provide us some training on investigating and prosecuting tech crimes so we are continuing to focus on that effort to build our capacity. It's a process but we are continuing to focus on it.

Agenda Item 8 – Report from Jim Owens on information motorists are required to exchange at traffic accident scenes and potential risks from disclosure of personal identifying information. (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. Owens:
Thank you, Madame Chairman. What is required of drivers is actually spelled out in Nevada NRS 484E.030. Basically, what you are required to share is your name, your address, and license plate number. By statute, that's all that you have to share. We take reports at LVMPD, we take reports that have a lot more information than that. Those reports are then put into our records bureau and if the person you had an accident with requests a copy of that report, all of the personal information is redacted from the other person so you won't have access to that. We do have a posting on our website – an example of a drivers' exchange of information sheet that people can check on our website although the information sheet that we offer up contains significantly more information than what is mandated by the statute. The statute is very simple. Obviously, it's helpful to you if you can get some additional information such as an insurance carrier, policy numbers, that type of thing.

General Masto:
Can you put in context why we've asked you to provide this information for us today?

Mr. Owens:
I imagine it's because recently LVMPD instituted a new policy that our officers no longer respond to property damage only accidents. If there is an injury involved, we respond or if there's a problem, the officers will respond to resolve it, clear the road of debris, that type of thing or if one of the parties is not cooperating with the other, we will respond to help. As a rule, we are trying to move away from responding to a simple property damage only accident.

General Masto'
Are you aware with the new policy now that anybody is taking advantage in scamming people by trying to gather more information from them than necessary or showing up to the scene of an accident and representing that they are there to address and care for the concerns as it relates to the accident?

Mr. Owens:

There have been reports that people will show up to accidents and offer to take this information for you. Some claim to be attorneys, others not just help them through the process. That certainly could be an issue if people divulge too much of their personal information such as full name, date of birth, social security number, that's the golden triangle for them.

General Masto:
So, for that reason, you talked a little about Metro pushing information out at least having on your website a driver exchange sheet to let individuals know that if they in an accident that this is the information they should exchange. Is that the intent of that driver's exchange sheet and being on your website?

Mr. Owens:
Yes, it's to help people. This is the type of information you should ask for. What you can ask for and what are mandated are two different things on our page on the website, it does not ask you to get their social security number or an actual date of birth but one does have to be careful.

General Masto:
Is there any public awareness campaign that Metro is undertaking to get that information out to individuals and I ask that because I want to offer our office and our resources the ability to also push that information out to educate drivers?

Mr. Owens:
I'm not sure how much we've pushed out to the public on this. I'd need to refer it to the PIO's office to find out for sure.

General Masto:
Any questions or comments from Board Members?

Mr. Berghel:
Jim, it's my understanding that no information beyond the three pieces that you specified – name, address and the license plate number are required by law, is that right?

Mr. Owens:
Name, address, license plate number is the requirement.

Mr. Berghel:
So, that would apply to information requested by law enforcement as well as information requested by another motorist?

Mr. Owens:
Law enforcement is a little bit different. There's a stipulation here in the section, basically in the 484E.030, 'the person shall give his or her name, address, and the registration number of the vehicle the driver is driving and, shall upon request and if available, exhibit his or her license to operate a motor vehicle to any person injured in such accident or to the driver or occupant of or person attending any vehicle or their property damaged in such accidents". They can ask to see your license; it doesn't say you have to give it to them. You just have to

exhibit your driver's license to them. This is just the other person at the accident. The next Subsection B – gives such information and upon request, manually surrender such license to any police officer at the scene of the accident or who is investigating the accident. There is a separation. It's a mandate that you have to show your license to the police officer investigating the accident but not until the person you are involved with.

General Masto:
Any other questions? Thank you, Mr. Owens.

Agenda Item 9 – Discussion and possible action on recommendations from Technical Privacy Subcommittee:

Mr. Berghel:
Some of these, I'll go through them roughly in order. Some of them have not been recommended to the Technical Crime Advisory Board at this point. They are under consideration by the Privacy Subcommittee that includes the first one, legislation to prohibit automatic license plate reader systems.

A. Legislation to prohibit Automatic License Plate Reader Systems in Nevada.
It turns out that this is quite a can of worms. It has some weighty constitutional issues and it is my understanding the laws that were passed in Utah and Arkansas have been contested and the one in Arkansas, I believe, is before their Supreme Court. The law in Utah, I believe, was withdrawn by the legislature. There is some opportunity there for the State of Nevada to try to meander through the constitutional labyrinth and see if there is a protection or two that's available to the citizenry and we'll report back on that at a later meeting.

B. Legislation to require full disclosure when metadata is captured and retained by government entities in Nevada.
We have no position at this point that has been deferred to a subsequent meeting.

C. Legislation on proposed telematics black box legislation.
The concern that I brought before the Privacy Subcommittee was that these are becoming ubiquitous and there are privacy implications in having all of these devices connected. In addition to that, there are some security implications and by that, I mean physical security implications. For example, the black box is connected to the car computer as is the tire pressure monitoring system and the blue tooth connections that are available on the steering wheel hub to operate your radio and that sort of thing. This is from the point of view of a digital security specialist; every automobile is an umbrella of radio frequency. Of course, since radio frequencies don't obey property lines, this is an opportunity for hacking. At the micro level, there are instructions in the car computer such as lock up front wheel brake, you don't want those kind of things to be invoked at speed and so, when you open the access to the car computer whether it's the black boxes or any other telematics device, you have a privacy implication and you also have a physical security implication because if this gets hacked, it can result in loss of life and limb. We are studying that now and hope to be able to report back to you in the near future.

D. Legislation to expand the news shield privilege under NRS 49.275 to address gaps created by technology

The Shield Law is in your back up. A lot of these have back up items but they're not fully gestated at this point. The point of the Shield Law modification revision was this: Modern journalism is no longer restricted to the traditional journalistic employers, by that I mean, publishers, newspapers, electronic media outlets like television news rooms and the like. Now, we are seeing blogospheres delivering fairly high quality and in some cases, accurate reporting and the Subcommittee would like to remind the Board that many of the accepted online venues for news coverage, such as the Huffington Post and the blogospheres such as that are considered to be fairly reliable and useful. But they are not protected under the Nevada Statute as it now stands so we've proposed a revision to that statute that seeks to incorporate coverage to those who act as journalists not based on the nature of the employment relationship. I'm not a lawyer so I'm going to have to leave it to Madame Chair's discretion whether this is something that she would feel comfortable in supporting. It is our feeling that is, the Privacy Subcommittee's feeling, that in the absence of a federal Shield Law, we are still, I would remind all of us that are non-lawyers, we are still operating under Brandsburg which means there is no federal protection at all. It's left to the states to protect journalism. We see cases all of the time these days where the federal government has decided to suppress a journalist for covering some piece of newsworthy information or other. To the extent that it is possible to protect the journalists, it has to be done at the state level. We propose that the already excellent Nevada statute be further enhanced. Since that is a recommendation to the Board, I'll pause here if any of you have questions or comments.

General Masto:
So, the way I am looking at Agenda Item Number D in the actual proposal is the law already exists and the enhancement is to include or broaden it to include technology and the journalism that occurs through blogging in the new technology and the new medium, is that correct?

Mr. Berghel:
Yes, it's worded in such a way that we don't have to be technology focused because by the time we get the new statute passed, the technology will have changed again. We've endeavored in this proposed statute revision to expand the coverage on the basis of the function of the journalist not the particular manner or means by which they apply their journalistic skills.

Mr. Owens:
I have on question. I am certainly not an attorney but as a law enforcement representative, I would just have a concern – would this then give any blogger the right to be shielded pretty much anybody that posts anything for others to see that we would not be able to require them to give up sources or specific information.

Mr. Berghel:
Yes, the intent is that if a person is engaged in journalism and the definition here is provided in that first paragraph, so to the extent that a person is doing that, yes, they would be covered. Whether the activity is represented by some kind of newsprint or an online source.

Mr. Owens:
At face value, that isn't something that I'd be wanting to support from the law enforcement aspect of it.

General Masto:
I have a follow-up – did you reach out or talk with the press association regarding this.

Mr. Berghel:
Yes, Madame Chair, we did engage them. Brett, what was Brian's last name?

Mr. Kandt:
Barry Smith with the Nevada Press Association.

Mr. Berghel:
Please let Barry address the question that was just raised.

Mr. Smith:
I am Barry Smith, Director of the Nevada Press Association. I was fortunate enough and appreciate the Privacy Subcommittee letting me talk to them a couple of times. This is an issue very near and dear to the Press Association where this came from originally. We do have, in Nevada, one of the best Shield Laws in the nation. It does, as I told them, for 90 percent of my members, we're covered and we're covered very well so our point of view is that we are kind of hesitant to touch it.

On the other hand, I did express to the Subcommittee that this is a good way to go about looking at this issue. Not so much who is covered but what their intent is, what activity that they are actually doing. As you see in the language, it really changes it from covering a journalist to covering acts of journalism. I think it's a good approach from the Press Association's point of view, for the most part, as I say, most of our members are newspapers covered explicitly by the statute. I do have members though and I expect I will more members in the future who are not specifically defined in that statute as being covered by the Shield Law. So far, there have been a couple of instances in the state and district court level where the issue has come up and the judges have pretty liberally construed that if it looks like a newspaper, the quote I used is just because you are reading a book on a Kindle doesn't mean it's not a book. So just because you are reading a newspaper online, doesn't mean it's not a newspaper. But, that's not the way the statute reads. That's my point of view on it and I'll be glad to answer any questions you have about it.

General Masto:
Thank you. I guess let me ask you a question that relates to what Jim Owens just brought up. I guess the question I would have for the press association is do you see a distinction when we define journalism between your membership and maybe, somebody who is blogging online their journal or topical information but they are not related to per say a news organization. Is there a distinction in your mind or with respect to your association?

Mr. Smith:

Yes, I do think there is a distinction. It's becoming more blurred all the time and this was pointed out some of the most popular, best read, news sources in the country. It would not qualify as a newspaper or TV or broadcast, radio broadcast organization. So, it does get into a very tricky question of defining what is journalism and that's why, on the federal level, so far, and there have been several attempts, it has not been defined, it is difficult to say what a person is doing. Once you get into when you are hired, there is a presumption of some level of education, training, skill, responsibility, those kinds of things. That's why the shorthand has generally been you work for a media organization. Is that helpful at all?

General Masto:
Yes, thank you. Any further comments or questions?

Mr. Owens:
Just for some clarification for me so according to this, if a blogger or a person who posts on their Facebook to his fellow criminal his particular gang, these are the crimes, they take pictures of some of the things they've done because it has interest to a particular segment of the public, his fellow gang members, so that's now protected and we can't bring him or require him to provide any additional information other than what he has posted?

Mr. Berghel:
Jim, I'm not an attorney. My guess is that that is the kind of thing that would be resolved by a court. That's part of the process. The intent here, I think, is, as Barry has pointed out, is pretty clear. The future of journalism for especially the younger set does not involve traditional means. That is many of us no longer subscribe to a newspapers or magazines for that matter but we are vociferous consumers of online content and if for no other reason than economic incentives, the spoils will go to the aggressive in attracting businesses to the states that provide these kinds of Shield Laws. That is, if you want a Huffington Post to start up in your midst, this kind of Shield Law that we proposed would be an incentive over a state that doesn't have this secure Shield Law. Now, when it comes to the details of how the laws are sorted out and how the prosecutors handle it, that's something, an issue that really should be left to an attorney. I'm not one.

General Masto:
Any other comments?

E. Legislation to amend NRS 205.473-.513, *inclusive*, "Unlawful Acts Regarding Computers and Information Service".

Mr. Berghel:
Legislation to amend the statute on computer abuse. I am actually drafting that. I'll give you a little background because I have nothing to propose at this time. The law itself was well intentioned but I presume written a very long time ago. The language is dated and I think it has serious issues. From a prosecutorial point of view, I would imagine it would be very difficult to enforce this law. I've taken the initiative to re-write it and it's probably, Brett, did you include a draft of my notes?

Mr. Kandt:

No, I did not, Professor, since it wasn't an item that had been approved by the Subcommittee yet, I had not.

Mr. Berghel:
OK, that's the right thing to do. It isn't ready for prime time. However, it's a fairly lengthy statute and I started with the best of intentions as a good non-lawyer and that is, don't start mucking around with things because there are implications that are carried through throughout the statues and we start changing definitions and so I approached it from modest perspective and just getting it to work, to hang together in a coherent whole was impossible. So, I just re-wrote it. I have no idea where this is in terms of its implications for NRS at this point. It needs to be carefully looked after by an attorney and I haven't got anyone on our Subcommittee to do that yet. That's the reason you are not seeing it yet. That's the background. I don't think minimalism is going to fix this particular problem.

F. Legislation to amend the statutory definition of "personal information" in NRS 603A.040.

Mr. Berghel:
Again, that was deferred. It turns out I'm very comfortable with the NIST definition of PII. I have absolutely no trouble with that. Of course, I didn't have any trouble with their last three or four versions. However, some of the Subcommittee members pointed out, they change it so often that it may not be in the state's interest to codify one of their versions and it probably wouldn't be passable to simply put a link in and say, Nevada follows NIST so we've decided to hold that off for a later date.

G. Legislation to amend the Nevada Constitution to establish an express right to privacy.

Mr. Berghel:
You will find this attached. We want to change Article 1, Section 1 after considerable discussion, we all agreed that we wanted to add privacy and thereby making our Article 1, Section 1 conform to other progressive states like California. However, at the insistence of Mr. Elste, we put privacy before happiness. From a logical point of view, it absolutely makes no difference. We recommend that to you for your consideration. Some of the members felt that there are better ways of going about this and one of them suggested that Montana has an excellent privacy clause in its constitution and I presented that to you here. The right of individual privacy is essential to the well-being of a free society and shall not be infringed without showing a compelling state interest and the Subcommittee felt that that was a very good way of putting it. However, that's not a minimalist approach and so while we all felt comfortable with that, we thought that from a practical point of view, it would be more likely that we would be able to get the Legislature to embrace the more minimal approach. I recommend that for your consideration, Madame Chair.

H. Proposed request for the Nevada Legislature to pass joint resolution calling on Nevada congressional delegation to expand online privacy rights under federal law.
Mr. Berghel:

It's lengthy so I won't read that here but I will give you some sense of the motivation behind it. We have seen in the last two or three years, a drama play out in Congress and the media regarding the warrantless surveillance undertaken by the NSA. Through Edward Snowden's revelations, via Glen Greenward and some other journalists, it turns out that this is kind of a hydra headed assault on the Fourth Amendment. As a matter of fact, as a non-attorney, my sense is that the Snowden revelations indicate that a good part of the central part of the Bill of Rights took the pipe on this. It seems like a lot of them are being tested. It didn't help, of course, when the head of the NSA, Michael Hayden, pointed out that the Fourth Amendment that the NSA uses doesn't have probable cause in it. With that kind of thing as a backdrop, we feel a strong recommendation to our federal congressional delegation to the effect that we want to encourage privacy to a paramount concern in future online legislation from this point on. So that resolution available for your consideration as well.

Mr. ?:

I have a couple of questions on the version you gave us for the change of the Nevada Constitution and simply add the words "and privacy". I guess my question would be not being an attorney, privacy means a lot of different things to a lot of different people and we certainly need to find out what exactly that means and then I have the second piece of paper that has to do with the joint resolution – do we all have this, Madam Chairman? I just had a concern, Hal, this was a joint resolution sent to the members of the 77th Session of the Nevada Legislature? Was that the past session or this the upcoming?

Mr. Berghel:
The upcoming.

Mr. ?:
I would have a question or a concern about this as well, it's talking about limiting this collection of information but at one point in the paragraph, it specifically states "we urge Congress to enact legislation ensuring that information about the lives and activities of citizens of the State of Nevada be collected and used only with continuing consent of the individual citizen concerned given openly, knowledgeably, and explicitly for specific identified purpose". What does that do to criminal investigations?

Mr. Berghel:
Again, you seem to feel that I'm more qualified in dealing with the law than I am. I would have to remind you, I've never taken a course in the law, so you are really asking the wrong person. I can tell you the motivation because I was present at all the discussions and I can tell you that this draft was written three very distinguished attorneys on the Sub-Committee. Those, I can comment about but as far as the interpretation of it, that's something for the lawyers to make good on. The other question you raised had to do with the insertion of the word "privacy".

Again, as a neophyte, it's my understanding that when such things are codified in the constitution or in the law, that they are interpreted by the courts and that the interpretations and meanings actually are a product of case law. That's a natural thing and to expect the constitution to handle all of the contingencies would be an unwarranted expectation. What we're saying in this is that the legislature in the State of

Nevada is going on record as saying that privacy is an important constitutional safeguard in this state. We are making that clear. How that is interpreted by courts is, of course, is something we have no control over. Does that answer your question?

Mr. ?:
It answers my question but doesn't address my concerns but you are right, it will play out in court. We'll go with that but I do have a concern on the second one and I would urge that the Board not just, I don't know if we are being asked to support each of these things that we are going to recommend to the governor that this Board supports these recommendations?

General Masto:
That's what I wanted clarification on. So, the first thing I wanted to know is – a through i – are those items that were voted on by the Subcommittee to bring forward for us to make a determination on? Which ones were actually action items by the Subcommittee to move forward to this Board for further action.

Mr. Berghel:
Thank you Madam Chair. The reason that a through i is on there is clerical. I think Brett included those to give you an idea of what we're doing. The action items are "d", "g" and "h". Is that correct, Brett?

Mr. Kandt:
That is correct. The last meeting of the Subcommittee was just last Friday, May 30th and out of an abundance of caution to provide the ability of the Board to act on any of these potential recommendations, I just included everything that was under the Subcommittee's consideration on the agenda.

General Masto:
Any further questions or comments regarding items a through i on Agenda Item 9?

Senator Ford:
A couple of questions – first off, Subsection g that looks to amend the Constitution express right of privacy. A question of research that I would like to propose or maybe the answer is already known, it seems to me and I don't do First Amendment law but my recollection is that our privacy laws under our Nevada Constitution quite terminus with those of the U.S. Constitution. That is, our Nevada courts construe privacy in the same way and to the same extent and limits as the federal courts under the U.S. Constitution. If that's an inaccurate statement that I've just made, and if so, then the question becomes do we need to amend the constitution to expressly indicate a right of privacy if our courts have already implied that right and it's been construed coterminous with the U.S. Constitution. Would Brett know the answer to that?

General Masto:
Before you answer, I would be curious knowing that there are attorneys on the Subcommittee if that issue came up.

Mr. Berghel:
Yes, it's my understanding that privacy is interpreted as falling under the penumbra of the Bill of Rights under the existing Supreme Court decisions. Again, I am not an attorney although if we have subsequent discussion about that, I think it would be wise for the Subcommittee's attorneys to be present to answer those questions. However, some of the states, California is the one I'm giving as an example, have added privacy to their constitution to stake out the territory, so to speak, make it clear that the state takes that responsibility to protect and safeguard the citizens' privacy as paramount it's right there with the protection of property and life and limb and happiness and everything else. Setting that out in such a way makes it more difficult for those who would seek to abrogate it. That was the intention from a non-legal point of view. That's why we decided to do it. Does that answer the question?

Senator Ford:
No, I don't think so – I think that ultimately I might need to see if Brett can give an answer to me on that because it seems to me that if spelling it out isn't really addressing the issue because it's already been construed in our courts coterminous and to the same extent that other enumerated fundamental rights, then I'd rather not have to entertain that. It's a difficult issue as you might imagine, legislating but it's even more difficult to get a constitutional amendment changed. I would be interested in knowing what the current state of the law is on that relevant to privacy. I don't know if we can get that before the next meeting or there's action going to be taken on this prior to that then that's another issue. Those are my concerns about Subsection G.

General Masto:
Brett, did you have a comment as well?

Mr. Kandt:
Certainly, a right to privacy whether it's expressed or implied in a constitution is still subject to interpretation and delineation by the courts. In addition, with regard to the Nevada Supreme Court construing privacy in various contexts under the Nevada Constitution has, in certain respects, primarily in the area of search and seizure, construed the rights of the individual to be greater and extended the protections to a greater extent under Nevada law, the Nevada Constitution, than has been construed by the U.S. Supreme Court under the U.S. Constitution.

Mr. Abney:
As we discuss this, I'm still not sure what we are being asked to do today. As we move forward with these discussions and my own two cents, I believe that on things like the Shield Law and certainly on things like amending the Nevada Constitution to establish an express right to "privacy", I feel like those two issues especially are way beyond the scope of the Technological Crime Advisory Committee.
I think things like the black box that we've been talking about - license plate readers, the warrant systems, I think those things are perfectly legitimate and things we need to talk about here. I know that technology moves fast and so we try to catch up with our laws and I think that's why we are here. To serve during the interim and get all the information we can and then, every two years, go to the Legislature and give them the best information

that we have. I'm not saying those issues aren't vitally important, I think privacy and what that means and the rights thereof is extremely important and I would love to sit in a committee room and hear legislators, like Senator Ford and others talk about that and go through those arguments but I feel that something so broad as amending the constitution to including that in such a nebulous manner, I believe, this is just one Board member's opinion, is beyond our scope here.

Senator Ford:
I was just going to say ditto what Tray just said actually. I wondered the same thing whether this was in the purview of the Technological Crime Committee. I wasn't going to mention it but Tray did so good for him. I just wanted to say ditto to that.

Mr. Berghel:
I don't disagree but I think it's useful for us all remember that there is difference between the way we self-organize and the way we get work done. The Subcommittee was specifically tasked to come up with ways of enhancing privacy for the citizens of Nevada. It just so happened that it was organized under the Technology Crimes Advisory Board. That doesn't detract from the fact that it is faithful to its charge. Ultimately, the recommendations are made to you, Madam Chair, the Attorney General.

General Masto:
Thank you. Any other further comments or questions regarding this topic. I can't disagree with the comments that I've heard here, today, so here's what we're going to do. With respect to the items D, G, and H, we're going to put those on hold, right now. Mr. Kandt and I will take a look at not only whether or not the Board has the authority to look into this particular area and whether we should be tasking the Subcommittee with that direction. We will also look at the general issue of legislation. Because I do know that by putting something like this on this committee, we also have federal partners and quite often, our federal partners sometimes are concerned about taking issue or voting on issues that may only pertain to state statutes and not federal statutes. That's why I'm always cautious when it comes to legislation itself. Traditionally, how we've handled this is if because we have such wonderful partners with the legislature and usually have an assembly representative and a senate representative, they, if they are interested in moving forward with any legislation or any issue that comes before this Board, they usually will handle it and move it forward at their own direction and discretion. We will, as a board, support it if it's an issue that we have voted on and said yes, we conceptually support that concept.
Really, it's a legislator that is going to introduce it and move forward and it's going to be their determination whether to do so or not. That's why I'm very cautious when it comes to legislation. Let's put those items on hold. We'll take a look at it and we'll also take a look at the tasks set for the Subcommittee without taking away the Subcommittee's teeth and ability to move forward with certain issues when it comes to privacy. Brett and I will take a look at that working with the Subcommittee. Then, we will come back to the board.

I. Proposed revisions to the State of Nevada Online Privacy Policy (http://nv.gov/privacy-policy/).

Any further questions on Agenda Item 9. If not, we will move to Agenda Item 10.

Agenda Item 10 – Discussion and possible action on the following additional proposals for legislation for the 78th (2015) Nevada Legislative Session:

A. Amending NRS 179.045 to authorize the application for and issuance of search warrants by electronic transmission.

General Masto:
Brett, can you identify how this legislation came to be on this agenda and before this Board. Is this legislation that you've put on or is this also from the Subcommittee.

Mr. Kandt:
At the last meeting of the Board, I brought up a proposal to look at NRS 179.045 which is the statute that provides for the application for and issuance of search warrants in Nevada, to consider updating the statute to allow for the use of technology. This Board recommended that that proposal be referred to the Technical Privacy Subcommittee. The Technical Privacy Subcommittee and if the Chair of that Subcommittee is ok for me representing this, at their meeting last Friday, May 30, 2014, expressed support for the concept of amending NRS 175.045 to allow for electronic transmissions in the application for and issuance of search warrants on the condition that appropriate safe guards for security and privacy could be identified and incorporated. The Subcommittee is willing to provide advice on implementation to the Nevada Legislature and perhaps, the Nevada Supreme Court. Earlier in the meeting today, you got a demonstration of one type of technology that is available from the Palentine Group and their electronic warrant interchange system. That's just one example but I wanted to give you an example of the type of technology that's out there and the fact that an increasing number of states are authorizing the use of technology to allow for the application for and issuance of search warrants by electronic transmission.

I think our federal partners are here. They can talk about their ability to utilize technology under the federal statutes that govern the issuance of search warrants. Nevertheless, it's something that I think we want to look at, here, in Nevada and updating our statute. Understanding of course, that any process does need to provide for the three elements of secured electronic transaction: authentication, integrity, and non-repudiation. Rather than getting into the details of what that would look like, what I am hoping is that based upon the Technological Privacy Subcommittee's expression of support, that this Board would support the concept of amending the statute to allow for the application for and issuance of search warrants by a secure electronic transmission. What I am proposing is that that authorization would specify that the Nevada Supreme Court could adopt rules, not inconsistent with the rules of the state to allow for that process. That's not unusual that the Nevada Supreme Court is granted rule making authority to adopt rules. They were granted that when it came to electronic filing. Now there's electronic filing of pleadings and documents in all our state courts pursuant to rules adopted by the Nevada Supreme Court. That's probably the appropriate way to go about it. Kentucky just did that. They just passed enabling legislation in this area in Kentucky and just specified that the Kentucky Supreme Court would adopt rules to provide the specifics. That's what I would hope this Board would do, take action to support amending our statute to enable the use of technology in the application for the issuance of search warrants by secure electronic transmission.

General Masto:
Any discussion by Board members on Agenda Item 10 A?

Mr. Owens:
From what I know and what I've read, this looks like a good idea, something that we would be certainly willing to support on the law enforcement side.

General Masto:
Any other comments?

Mr. Kandt:
I just wanted to reiterate, I had mentioned at the last Board meeting when I first broached this subject, I had reached out to the ACLU who indicated they had no opposition to this proposal. Pursuant to Senator Ford's request since the last meeting, I reached out to the NAACP, both in Reno and Las Vegas, they didn't specify any objection. I have shared this concept and this proposal with the Public Defenders and with the court system. I am trying to reach out to all the stakeholders and all the affected parties. As I indicated before, the Sheriffs and Chiefs Association and the state and local prosecutors had already signified their support for this concept.

Mr. Berghel:
I don't have, from the point of view the concept, a horse in this race. I don't represent law enforcement and I certainly don't have any experience with judicial side. From the point of view of technology which I do understand, you saw a demonstration that used 128 bit SSL encryption and I'd remind you that just four or five months ago, there was a major hack because a feeble encryption algorithm was embedded into the RSA implementation of this ____. That has yet to be sorted out. What that means is that while it might look secure, that appearance is illusory. The level of encryption used by the product that we saw was very inadequate from the point of view of the technical issues represented by the Subcommittee on Privacy. Secondly, you notice that the authentication was what we call "scrabbling". It was just a touch pad signature. Those are trivial to counterfeit and of this is being broadcast over RF so there are opportunities there for use that I think this Board wants to consider before they pass such a recommendation on to the Legislature.

General Masto;
Any other comments or questions? I guess one comment I have is because this express support for the concept came from the Privacy Subcommittee, were they addressing your concerns, Hal, when they put in there on the condition that appropriate safeguards for security and privacy could be identified and incorporated.

Mr. Berghel:
Thank you, Madam Chair, The position of the Subcommittee was that the general concept was not something that we thought we had any problem with but we couldn't see from the information that Brett provided us, how that personal privacy and security and reliability and authentication could be built into this in a nonintrusive way. Since we didn't have anything to work with and we couldn't comment on specific technology recommendations because there weren't any, the strongest recommendation we could say is we're not opposed to the concept. However, that doesn't mean that whatever manner or means the recommendation chooses to

take, is something that would meet with the Privacy Subcommittee's approval. We haven't seen anything yet.

General Masto:
The issue before the Board at this time would be whether or not there's interest to move forward in a motion to support the concept of the amending NRS 179.045 to allow for electronic transmissions on the condition that appropriate safeguards for security and privacy could be identified and incorporated.

Mr. Abney:
I can make that motion. Senator Ford: I second the motion.

General Masto:
Any further discussion? Hearing none, all those in favor signify by saying I. Those opposed? The motion has been unanimously approved.

Mr. Ford:
I have another appointment and have to leave the call. I just wanted to let you know.

General Masto:
Thank you for your participation. Brett, does that affect our quorum and or our ability to take action on the next item?

Mr. Kandt:
Yes, it does but I didn't anticipate action on the next item. If it is OK with you, I'll just provide some information to the Board, just as an informational item.

B. Amending NRS 179.410-.530 regarding the interception of electronic communication, exception for a barricade or hostage situation, and use of pen registers to reference 18 U.S.C. § 2703 and §§ 3121-3127 as amended.

This next item talks about amending other statutes in the same chapter of NRS 179, specifically, the statutes .410 through .530. These are the statutes that deal with the interception of electronic communications. Right now, those statutes are all drafted with reference to a wire communication or an oral communication. In our conversations with our law enforcement partners on the local level, especially Las Vegas Metro, it's just been demonstrated that this, once again, is an example of where these statutes need to be updated so that these statutes can address the process for gaining court approval to intercept an electronic communication in the general sense.

We are working on some draft language, it's not finalized now. I just wanted this Board to be aware of that. Also, to possibly create a specific express statutory exception for those situations in which there is a barricade or hostage situation.

Finally, with regard to the use of pen registers, that statute, right now, simply references 18 U.S.C. § 3121 through §§3127 but the language of the statute. Right now, the pen register or trap and trace devices, we are talking about NRS 179.530, specifies that the process by

which the state can issue orders authorizing the use of pen register or trap and trace device have to be under the circumstances and upon the conditions prescribed by 18 U.S.C. §§ 3121-3127 as those provisions existed on July 1, 1989. That is when this statute was enacted.

The fact of the matter is since July 1, 1989, those federal statutes have been amended many times. In addition, 18 U.S.C. §2703 has been enacted which provides for the contents of stored electronic communications and accessing that data. That statute is not even referenced here so I think one recommendation will be to amend that statute so the reference is made to all the applicable federal statutes and they say as they are amended so to the extent those statutes are amended from time to time by the U.S. Congress that that be incorporated into our state statutes that follows those federal statutes.

Those are just some things we are looking at. I don't know if Mr. Owens wants to further elaborate since a lot of this came out of his shop and issues they have encountered but once again, we are looking at updating these statutes to account for the use of technology and I'll continue to keep the Board posted.

Mr. Owens:
I don't need to elaborate but I do need to thank you for your help with this. This is a critical need that we have here, particularly in these hostage or barricade situations. We appreciate any help you can give us with this.

General Masto:
Any further comments or questions?

Agenda Item 11 – 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.

No additional comments or discussion.

Agenda Item 12 – Discussion and possible action on time and location of next meeting.

General Masto:
I would recommend that we continue to ask Brett Kandt to work and coordinate the times, meetings, locations for the next meeting.

General Masto:
Brett, do you have anything to add?

Mr. Kandt: No, Madam Chair, once again because we have lost quorum, you can't designate a specific time and place for the next meeting. I will coordinate that with the schedules of all the Board members.

Agenda Item 13 – Discussion and possible action on future agenda items.

General Masto:

If any member has thoughts now, they can let us know or as always, send an email to Mr. Kandt.

Agenda Item 14 – Public Comment.

General Masto:
Is there any member of the public who would like to address the Board in Las Vegas at this time? Seeing and hearing no one, anyone in Carson City a member of the public who would like to address the Board at this time? Seeing and hearing no one, we will move on to Agenda Item 15.

Agenda Item 15 – Discussion and possible action on adjournment.

General Masto: We are adjourned.