TECHNOLOGICAL CRIME ADVISORY BOARD

MINUTES OF THE MEETING

March 6, 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

The Technological Crime Advisory Board was called to order at 2:00 pm on Thursday, March 6, 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)
Dennis Cobb, Co-Director of the UNLV Identity Theft and Financial Fraud Research & Operations Center.
State Assemblyman Paul Anderson

Advisory Board Members Present in Carson City:
Kyle Burns, Resident Agent in Charge, Homeland Security Investigations
David Gustafson, State Chief Information Officer, Enterprise IT Services
Nevada State Senator Aaron Ford (via phone)

Advisory Board Members Absent:
Professor Hal Berghel, University of Nevada, Las Vegas
Tray Abney, Reno/Sparks Chamber of Commerce
William Uffelman, President and Chief Executive Officer, Nevada Bankers Association

Brett Kandt advised that Mr. Balaam, Mr. Bogden and Mr. Shields are no longer on the Board.

Staff Members Present:
Brett Kandt, Advisory Board Executive Director

Others Present:
Manita Rawat, Dwayne Morris Agency, LLP, Las Vegas, NV

Jack Williams, President, ERAD Group, Inc.

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.

This is the time for members of the Public to address the Board. There will also be a second opportunity at the end of this agenda. Are there any members of the public present that would like to address the Board at this time? No public comment.

Agenda Item 3 – Discussion and possible action on approval of September 12, 2013, meeting minutes.

Mr. Owens made a motion to approve the minutes. Mr. Cobb seconded the motion. The minutes were unanimously approved.

Agenda Item 4 – Presentation on patent trolling from Manita Rawat, Duane Morris LLP, Las Vegas.

Manita Rawat introduced herself and thanked the group for allowing her to come and talk about patent trolling. She is a registered patent attorney and an associate with the law firm of Duane Morris in Las Vegas.

The first thing is patent law is actually under the purview of the federal government. It's a constitutional right to own and have patents under Article 1, Section 8, Clause 8 of the U.S. Constitution. It gives Congress the power to enact laws pertaining to patent rights in the United States. Those rights are under Title 35 of the United States Code.

Congress, many years ago, created the United States Patent and Trademark Office which is the entity where one would file and prosecute a patent application and it would be obtained through the patent office. Also, the Patent Office came up with the manual of patenting examining procedure which we call the MPEP which is what the examiners at the U.S. PTO use to examine the patents and to eventually, approve them.

Two years ago, we had the American Invents Act which was enacted into law which had modified the patent system in the United States. We used to be a first-to-invent country in that the person who conceived and reduced the invention to practice was the rightful owner of a patent. In 2013, that changed. Now, it is the first-to-file so it's a race to the USPTO. Whoever files the patent application first will be the rightful owner of the patent.

There are three types of patents: there are utility patents which are processes, machines, articles of manufacturers and composition of matters. Then we have design

patents so that could be the actual design of the IPhone and when it's a design patent, we are not claiming the functional aspect of it but more of the aesthetic aspect of it. Then there are plant patents and those are variety of new plants that were produced.

There are different types of entities that will seek patent protection. One that's commonly seen is technology and scientific companies like Microsoft and IBM. More importantly, companies here in Nevada like IGT and Bally Gaming. These companies have research and development capabilities. They usually do the R & D in house and they file and prosecute the patent applications whether it's with the USPTO or foreign patents in trademark offices.

Other companies that seek patent protection are service companies so they may be companies that may not have R & D facilities or capabilities in-house but they've come up with a product that they use as part of their services and they patent that product. Universities, public and private also seek patent protection on the technology that they develop in-house. It's a really good revenue generating source for universities because they can license their technology out to private entities and receive a licensing royalty fee based on that. Government entities, the United States Air Force, Department of Defense, NASA, file patent applications as well. A lot of non-profit organizations have research and development capabilities. They do a lot of research and technology in-house and file patent applications on that. Similar to the universities and the government entities, they do it to hopefully have licensing opportunities as a way to generate revenue.

Here's where the patent assertion entities come in, aka patent trolls or non-practicing entities who don't have research and development capabilities nor do they develop a product that is being used out in the market place. What they do is purchase the patent rights to products that are already out there in the market place. They purchase these patents from solo inventors who have filed a patent or maybe small companies that have recently gone bankrupt or dissolved companies but do not use or manufacture the inventions covered under patent. They have a different approach. All of these entities, as a whole, whether they are a manufacturer or a patent assertion entity, have a right to enforce their patents. When you file a patent infringement action, it is in federal court because it's a federal question.

They have a right to go after competitors, for example, so if you see a competitor out there who has a product that is similar to a product that you have a patent on, you have the right to send a cease and desist letter, initially, notifying the potential patent infringer that they are potentially infringing on the patent. In order to resolve a lawsuit, they can enter into a licensing agreement and a settlement agreement. If that doesn't go well, then a lawsuit is filed in federal court.

Patent assertion entities are different because they are not out there in the market place with products or services. Because of the different incentive, they take a different approach to who they go after.

The patent assertion entities realized that it was getting expensive to go after well-funded companies. What they found was to go after the customers they are the ones who are using the products. They know these customers could be small business owners here in Nevada who probably aren't familiar with the patent process. They don't have deep pockets so when they get a cease and desist letter, they are going to cave in and say, we'll pay you $10,000 because it could cost us potentially $2 million to fight this in litigation. It's a quick settlement. What the patent assertion entities realize is that was a good approach but then it was high volume. We are going to go after as many potential customers as they possibly can and get a good rate of return on that.

Nevada is unique in that a lot of entities that could fall under concerned customers are casinos.

What companies like Microsoft and IBM saw was that these patent assertion entities were going after their customers. Customers are pretty big to their business so what they started to do was to try to protect their customers which easy to do if Microsoft was sued on the same patent and they settled the case with the patent assertion entity, and two years later this same patent assertion entity files a lawsuit against one of Microsoft's customers, it was easy to do in that case because they had already settled the lawsuit on the same patents with the manufacturer so there was probably a licensing agreement. In that licensing agreement there was a clause that provided protection to customers. If they went after their customers, they are protected under use theories, whatever language they use in the licensing agreement. In that situation, if they went after a customer and there was already a licensing or settlement agreement in place, the manufacturers like Microsoft could come in and file a lawsuit for breach of contract.

Some patent assertion entities picked up on this and decided let's not even go after the manufacturers, let's go after the customers. What had happened was there was a lawsuit, *Arris Group, Inc. v British Telecommunications*, I won't go into detail with this case but what had happened with the facts of this case was there was a customer of Arris Group, Capital One, who was using Arris Group's products. British Telecommunications had sent the customer a cease and desist letter saying you are infringing on our patent. The customer immediately notified the manufacturer that they had received the cease and desist letter but the products that they were using essentially the products that were purchased from you. They were a pretty significant customer for the Arris Group. In this case, they were negotiating for about two years after the cease and desist letter. Arris Group had become involved and said they are a customer, we developed the product. Arris Group filed a declaratory judgment action in federal court asserting invalidity of the patents so they went after the patents. They were told by the district court they had no standing; there was never an action against you. The federal circuit, this is called the customer exception where the federal circuit said that even though they weren't a direct party to any pending litigation or potential litigation, they were protecting a customer which gave them standing to file a lawsuit on

behalf of the customers. Manufacturers were seeing Google, Microsoft, SAP; they are now doing this on behalf of some of their very important customers.

What other states are doing and what Nevada has done, and every state has this, is we have consumer protection laws. We have our state versions of the UCC then we also have, in Nevada, particularly, we have NRS 598 which covers deceptive trade practices. That is what states are doing to protect customers.

Attorneys general in various states have filed lawsuits against patent assertion entities under whatever deceptive trade practices laws that those states have. There's a question as to whether those apply to cease and desist letters and whether they apply to patent cases as a whole. Vermont was the leading state in this area and they actually amended their consumer protection act to include acts that could be conducted by patent assertion entities.

They amended what includes a threat of bad faith. The bad faith that they required is that there be specificity in these cease and desist letters. These letters are very vague. They just say you're infringing on our patent. They don't identify the claims of the patent that is being infringed and they don't identify what the potential infringer has done. One of the things that Vermont has required now under their amendment is that there is specificity as to how infringement occurs in that particular case. They've also been prevented from demanding excessive licensing fees. Many times, customers don't know what a reasonable amount is for a licensing fee. The other thing that is pretty important is they have to now provide a reasonable deadline for payment. Many times, when a customer receives a cease and desist letter, they'll have 24 to 48 hours to make payments which gives the customer no time to consider what a reasonable amount to pay is or should they hire an attorney.

General Masto:
When you are talking about customers, you are actually talking about businesses that are using a technology that is really instrumental to carrying out their business. When they are challenged by an entity like this, it is not just a matter of them paying over the fees or trying to understand what is going on. It is challenging some sort of instrument they are using to carry on the functions of the business that could be detrimental to them if they go to some sort of litigation and the court rules against them.

That is what we are talking about here and why we are so concerned about the letters that are sent out whether they are fair, they are not deceptive and the businesses have an understanding of what is being asked of them. It is detrimental to them carrying out their business in the future.

Mr. Cobb:
I just wanted to add to that, that a lot of times there's an assumption which is a very safe assumption that when you buy a fax machine that has a scanner in it, that the technology that is wrapped up in that, has already been taken care of in the patent process or licensing process. A lot of these folks who are end user business owners

are being shocked that they bought something that wasn't truly licensed properly or they have the assumption that it was.

Ms. Rawat:
There is a lawsuit going on right now in Nevada that is impacting the casinos which is public knowledge because it is federal filing. The casinos have purchased display systems through whether it's Samsung, Toshiba. You can walk into a casino and you can see the big screens everywhere or even the conference centers will have display systems. The airport has display signage that they are using.

There is a patent assertion entity that owns a few patents on display systems and signage. They have now filed lawsuits against various entities in Nevada for using these display systems. It gets a little tricky because it's not so plain and simple in that a customer purchases a product and then uses it. They may modify it so they may purchase a display system but may couple a laptop to it or a small processing device so when there is some sort of indemnity clause, it doesn't cover modifications. Sometimes, those modifications may be covered under the claims of the patent. It's not cut and dried.

You purchase the product and are using the product as is. There could be modifications that can be made by the customer. You or I would buy a laptop computer and just use it. When you are a big company using display signs, you may modify it; you may have in-house engineers that can make certain modifications that could still potentially infringe under the patent. When the manufacturers are sued and have entered into a licensing agreement with the patentee, they cover the modifications. Sometimes the modifications aren't envisioned as being potentially threatened under a lawsuit. They are not thinking that way in a licensing agreement. Now the manufacturers have gone back and as a customer, you may negotiate different uses or modifications to be covered under various indemnification clauses.

At the federal level, we are getting help from Congress. HR 3309 and Senate Bill 1720 which is the Innovation Act, have passed in the House. It goes along with what Vermont has done requiring specificity when alleging infringement in a lawsuit. What is important is Vermont's statute made specificity a requirement in the cease and desist letter. What federal law does is require specificity in the pleadings requirement. Once it is filed in federal court, the complaint has to provide specificity as to the alleged infringement. It doesn't address anything prior to the lawsuit such as when a cease and desist letter is sent out.

It makes patent ownership more transparent requiring information about the entity that is bringing forth the patent infringement lawsuit. It makes losing plaintiffs pay. If you lose a patent infringement lawsuit, plaintiff has the right to recoup payment. It provides discovery options that could help to prevent delays in the discovery process. This is all after a lawsuit has been filed. It doesn't address anything before a lawsuit is filed. I don't know how much that is going to protect customers because they may not even get

to the lawsuit stage because they try to resolve it as soon as they receive a cease and desist letter.

The attorney generals from each of the states, including our State of Nevada Attorney General, Catherine Masto, sent a letter to Congress letting them know that this is great; I believe you have a copy of it. In that letter, they address concerns and amendments that they want enacted to protect the states. The federal legislation has been passed in the House with those points that I discussed. We are hoping these amendments will come in in the Senate bill. The confirmation of state enforcement authority which is at the level of the cease and desist letter once the cease and desist letter is sent out. If there are state laws enacted to protect at that stage because again, the federal level only protects once a lawsuit has been filed or a complaint is being filed that only addresses requirements for the complaint, this allows states to say we want authority as to what can be done prior to that stage. Clarification of state court jurisdiction, if states such as Vermont have a statute in place, states they want protection to file a lawsuit on behalf of the customer without a federal lawsuit in place.

Further to the transparency of the patentees, we want to know who those patent owners are. Many times, you get a letter and look up the company name and find no information on it. We want to know if they are patent assertion entities or really manufacturers who have products out there on the market. We want to prevent this going on in each of the states.

I wanted to tie in some solutions you are considering here, in the State of Nevada. One is to amend NRS 598, make it similar to Vermont law.

We want to avoid federal preemption and because of what is going on in Vermont, we want to consider the First Amendment issues and we want to write a law that is not going to impede on someone's First Amendment rights.

Any questions?

General Masto:
I appreciate the presentation. Let me just say because of what has been happening in Vermont, and I have been aware of this issue over the course of the past two years, it has really heated up. On a regular basis, we are complaint-driven in my office so I monitor the complaints that come in on a regular basis to see the categories of alleged fraud that is occurring. I have not seen a complaint come in to my office on patent trolls which is interesting to me but maybe they don't know where to go.

We started reaching out to the communities and talking to some folks. We talked to a national business that is concerned about what is happening here. Our office is happy to look at this but we really haven't received any local businesses that have complained and wanted us to take action. It makes me concerned that (1) that they are just automatically settling or negotiating and giving them money out there, and, (2) this larger company went back and talked to some folks and gave me a list of maybe some

of the small businesses that claim to have this sort of issue. There really was not more than ten that I saw.

This is fascinating to me and it may be because it's an educational issue that the companies are getting these cease and desist letters and maybe taking them to private attorneys or figuring out how to address or deal with them personally without thinking that this might be a consumer protection issue to bring to the Attorney General. I guess for lack of a better word, we can use all the help we can get to get word out that if that is happening to some of our small businesses, and we will do the outreach, particularly to our chambers, that they just need to come to our office and file a complaint so we can take a look at what's going on. We absolutely would be there to protect them if these companies are running afoul of our existing statutes as it is.

With that said, I am concerned with the federal legislation and that's why we did sign on to that letter because I am always concerned about federal preemption. Not allowing the states, particularly the Attorney Generals who have the exclusive jurisdiction to handle unfair, deceptive trade practices to continue to protect their constituents if a federal law comes along and wipes us out of that type of enforcement and protection. We will continue to ensure that we have that opportunity and that authority to protect our constituents under our state laws. I will always fight that federal preemption. We are monitoring that legislation as it moves forward to make sure and talking with our delegation as well.

Assemblyman Anderson:
I could certainly give you a list of probably five entities that we have worked with on the tech side of things that have received letters, myself being one, which was specifically in regards to the scanning, copying, fax multi-function printer that everyone has in an office. We also had a CPA firm which was fairly large that was part of the customization idea that the software that they used had the ability to do customizations that allegedly infringed upon a process patent that was for a paperless deal.

We've seen a lot of them and I guess my questions are sort of in your addressing some of the solutions. First, what should we advise our consumers to do. What happens if you just ignore it or what happens if they go down the road. Are these loopholes that they are using or are they legitimate laws that they are following to gain the leverage.

Ms. Rawat:
The legitimate law is when you own a patent; you have a right to enforce the patent. If you see potential infringers, you have a right to go after them. They send a very broad letter, even the pleadings requirement when you file a patent infringement complaint; you don't need to identify the claims of the patent that are being infringed. You don't need to identify how the asserted product is infringing on the claim. It's just a notice of pleadings. Discovery is where you address that issue. They are doing everything legally that they can do – send a broad letter putting you on notice. Usually, they follow up saying they just want a payment; do they specify a payment in the letter?

Assemblyman Anderson:
There was a specific payment, something similar to $3,500, $5,000, somewhere in that range for a fax machine that probably cost $800. When we started to see several of them crop up across our client base, we obviously got more concerned.

They are not obligated to do anything but you could require them to provide clarification as to why you believe we're infringing because we don't really understand by your letter. You have a right to ask that. They have no obligation to fulfill that. They can tell you that they believe it is and that is something that if they file a lawsuit, then they figure it out during discovery.

Assemblyman Anderson:
If a consumer is in this situation, the recommended steps would be to immediately seek counsel or should we send them to the Attorney General's office to file a statement of concern.

Ms. Rawat:
I would notify the Attorney General's office and state that this could be a potential violation of NRS 598. Let the company know that you have notified the Attorney General's office. You could ask them to provide more information as to why there is infringement. For $5,000, I wouldn't recommend getting a patent lawyer involved but if it's a substantial amount, you may want to have a patent lawyer respond to the cease and desist letter.

Senator Ford:
I just wanted to commend her on the presentation and say very well done.

Ms. Rawat:
Thank you, Senator Ford. I put my contact information in the slide presentation at the end if there is anything I can help out with in the future, especially with the Attorney General's office or in terms of drafting the bill; if Nevada considers that, please feel free to contact me. I would be happy to help.

General Masto:
Thank you, we appreciate you being here.

Agenda Item 5 – Presentation on the money laundering risks of prepaid access and mobile devices from Jack Williams, President, ERAD Group, Inc.

General Masto:
Introduces Mr. Williams from ERAD Group, Inc.

Mr. Williams:
I don't think that when we sat in this room a few years ago that we thought or even had the vision that the Attorney General had that prepaid cards would become what they are

today. I am the inventor of the prepaid card. I introduced the very first gift card in 1993. Today, I sit on a variety of committees, either at the federal level or the Texas level.

I work with a variety of law enforcement as they look to wind down various cases. What we are going to talk about today is SB 82 and it's really the implementation and what it means to you, how to give you a flavor of what's happened in this universe because you are on the point of the spear.

This happened in 30 years – you remember the old brick phone that you used to have? That was $3,000 that you had to pay for it and it only worked for about a quarter of a mile so it really was something kind of unusual but it happened in 30 years that we are talking about a period of 20 years. I never thought that this would really come the circle that it has.

Let's look at what has happened and think of it in these terms. Today, to give you an idea of prepaid cards in the United States, one of the big advisory firms thinks that the open loop value of cards loaded in just the United States is about $3.15 billion. You add roughly the same amount or a little more in what they call closed loop gift cards, you are getting about $600 billion in the United States in prepaid cards. The concept of prepaid used and money laundering activities is not in its infancy, it is pretty much in a mature environment. The sex and human traffickers and cartels and the terrorists have all found that prepaid cards are a very quick, anonymous, easy way to move money. Terror cells can be financed from Yemen or Somalia only with a laptop computer with someone having internet access and can move funds from there to here and make them available, literally, in seconds.

One of the points that we talked about in the early development of SB 82 was how fast money can be moved from a cell phone. I would suggest today the cell phones moving money on the take downs that I am aware of, it's always someone there very quickly moving their fingers on their cell phone as opposed to maybe throwing drugs down the drain. The movement of money today can take place from anywhere in the world to anywhere in the world in seconds. That's what we will be talking about. We will also be going over how the various crime units have different uses for prepaid cards. The sex traffickers use prepaid cards in a different way than the human traffickers and how that evolves out and then how does what we've done mitigate some of that.

When you look at the size, it's a trillion dollars of money that is going to be loaded on these cards estimated in 2015. Cash seizures by the State of Texas have gone down roughly 52 percent. What's happening is the migration from cash over to plastic and being able to use that in a variety of ways.

When we talk about cards, there are two kinds of cards that we, in law enforcement, need to be aware of. One is those cards that are called branded or open loop like MasterCard, Visa, Discover, but soon there are new brands on the horizon that represent threats. China Union Pay, JCB, Amazon, PayPal. PayPal alone represents 232 million account holders, all of which are prepaid in the concept that money was

given to an account prior to its utilization. This is a global currency like no other currency in the world. Because it can be processed from anywhere and can be issued from anywhere, no one really cares about the limits we would impose if it's an offshore product. We look at the open loop – its global cash not just domestic cash. It works like any credit card. It works the same. You wouldn't know the difference.

Interesting thing on TSA, if we walk up to airport and we buy with cash, a ticket to Yemen, we'll hit every red flag in the TSA inventory. If they go in and buy a prepaid debit card and they use the same amount and buy the same ticket, it will look like credit card and will not hit any flags. These can be used as one time, they can be reloaded, there are approximately 150,000 locations in the United States where criminals are able secure funds and have it loaded on to prepaid cards. The funds can be transferred from one card to another card using internet or mobile phones. With the multiplicity of options, cards empower money laundering in ways that we have never anticipated. They can be generic, they can be personalized.

First, let's talk about closed loop cards: these are the cards that are most desired by the human traffickers. What has changed in the closed loop is a card that is issued by Walmart or K-Mart or Best Buy. It was the feeling of law enforcement that people did not really see the closed loop card as a threat. Today, closed loop cards have a liquidity of about 92% of the face value. There is a whole new industry has opened up that is fostered by the pay day lenders, the pawn shops, and even online. If you do a search on "sell my gift card", you'll see approximately 100 different locations websites that if you have a Walmart gift card or a Best Buy gift card, you can sell this card for 92 cents on the dollar. The liquidity of these cards has added to the utility of the criminal usage. They don't allow for international transmission of funds but they do allow for quick liquidity and access.

To give you an idea of how this works, this is a skimmer. This is a reader, writer skimmer that's approximately three inches by three inches by one inch. What the criminals are doing today to throw law enforcement off is they are taking legitimate cards. They are running them through a skimmer that looks like this and then they pick up a hotel room key that has a magnetic stripe on it and they run that magnetic stripe through the same unit. Now they have a card with the exact copy of what was on the master card that law enforcement would be able to see. They take this card and throw it away. Now we see take downs with 30, 40 even 100 hotel room keys.

You can go on EBay today and do a search and there are probably about 70 different sites that will sell you a credit card reader/writer. That is a device that while it's much bigger than this, it does hold 8,000 magnetic stripe data. You can go on EBay, they not only have a machine that reads and writes a card exactly, they even give you white plastic. Skimming of cards has become a very popular technique.

It was my vision of how to take this card and provide law enforcement with an easy system that allowed for law enforcement to be able to secure the value that is on the card, be able to know what it is in real time, and be able to see that here's a terminal

that is able, with push buttons, in two seconds can obtain the balance of a prepaid card, whether that card is a hotel room key or a legitimate card, it doesn't matter. It's the mag stripe that we're interrogating so not only can we take two or three seconds through a wireless mode or hard line, various connectivity options, but we are able to take and find 1) the balance that is associated with the card, and, 2) be able to freeze the value associated with the card for a period of a minimum of 96 hours. Then, using the same device or a computer at your desk, be able to call up a website that we would provide and be able to process that card, then seize the funds that are tied to that card and have those funds deposited into a bank account that was set up for that purpose.

Being able to secure funds in near real time, being able to know what the bad guy has on his cards and be able to stop him from moving that money from the card that you found onto another card, which should make it difficult forensically for me to trail.

Today, we think its $600 billion dollars are on prepaid cards. While the cartels and the sex traffickers don't report usage, I had no way of knowing for sure, there's a lot of people who think it's around $50 or $60 billion are used for illicit purposes in this country.

When you think about it, these cards can be processed from anywhere in the world to anywhere in the world. I thought it might be interesting to see how they are obtained at the point of arrest and be able to look at the ramifications of how that is.

These are the 6 categories that I have identified in my actions of how cards are found. Closed loop – that is a card that has a specific merchant name on the front that can be sold online. They are usually not personalized and they can't move money from one account to another.

Abandoned cards – we find many cards are abandoned. One individual had cards taped all over his body with clear moving tape. When he was stopped by an ICE agent, he told the agent he didn't know they got there. I don't know anything about them – I abandon them. This is kind of the way that cards are found.

Open loop, closed loop, abandoned property; sometimes we find that they are skimmed cards and hotel room keys. I've also been involved in cases where an agent called and he had 500 Subway cards. What they had done was they had stolen low value cards, Subway puts them right there on the checkout counter. They had stolen these cards and when I checked the value on the Subway cards, the cards had never been activated. They were just plastic as far as Subway was concerned but yet they had been skimmed with legitimate MasterCard and Visas. The only way is to be able to get them in real time and this is an idea of how cards are seen.

How are they used? These are the 7 silos that I have identified in my activities: Proceeds from the sale of drugs; sex trafficking; child pornography – these are the tools of trade for child pornographers; human trafficking; money laundering – good, old-fashioned-hide-my-money money laundering; ID theft with tax fraud; internet gambling;

and just others – dog fighting. What has driven prepaid cards to their importance today is square, you may have seen the devices that fit onto your smartphone, and it's a small device, approximately the same size that now is incorporated in your smartphone. Whether it's in prostitution or various forms of illegal activity, the square device has made it much easier.

These 7 categories are really the top line of how cards are found by and their usage. One of the areas that we should probably understand at this point is there's a misconception there's a limit to the amount of money that can be put on a card. The reality is there is no limit. It's my personal belief that the cartels own processors which is the hub of this wheel that we are going after. The Visa/MasterCard limit is basically $99 million on a transaction so having cards with three, four, and five million is not unreasonable. There is an Achilles heel and that is that there is always an audit trail. If we know what the card number is, we know how to go to the processor whether in the United States or overseas. We know how to find the forensics and from the forensics, we are able uncover far more information about the loading of accounts and how it was done.

This is the terminal that is on the forefront of the battle. It is a wireless terminal and I would be glad to show you a demonstration of how it works. My contact page has all the details to get in touch with me.

Mr. Owens:
How is it when the bad guys use this card, they can put $100,000 on the card?

Mr. Williams:
It's all at the processor level. There are three ingredients in every prepaid card. There's a program manager; there's an issuing institution, in most cases but not all; and there's a core processor. Somebody that has the database, the decrements, the value, does the reporting, and all the things that go with it. If you control the processor, you can put any amount on there. There's a case called Virtual Money, where an individual built his own in-house processing engine and he laundered, estimates are $1.1 billion over three years using prepaid cards. As long as you control the issuer, and you have a bank that is a cooperative bank or located outside of the United States that doesn't play by the same rules, then it's a task that only takes two or three seconds to put $100,000 or 1 million dollars onto a card's available balance.

Mr. Owens:
I'm the bad guy with a pocketful of money and I want to do this. I have to get $100,000 out of the country. I have the cash but I'm not that sophisticated. Then we have pimps coming into Las Vegas. How do I put that $100,000 on that card?

Mr. Williams:
You go into any one of 150,000 locations in the United States. Let's take this simple one – you go into any Walmart or a Walgreen's or CVS, hanging on the wall is what is called a grain dot money pack. It's a piece of paper about this size, hanging on a "J"

hook. You take it down, you walk up to the cashier, you give them your $500 that you want to load, you give them a $4.95 fee and then you take your money which has a number on it. It is the ability to pay cash to load your card at these various locations or if you have a cooperating processor, then it's much easier. They can do it all at one time.

Mr. Burns:
I am Kyle Burns with Homeland Security Investigations. I spent many years in headquarters in our finance unit working with FINCEN trying to get these cards classified as monetary instruments for currency reporting. We've long recognized this to be a major money laundering vulnerability. Do you have any intel on FINCEN is going to actually make this a monetary instrument? It's been in a proposed rule for what seems like three or four years.

Mr. Cobb:
I just wonder what your opinion is and this may be a little broad but I can envision this method eventually being superseded by cyber currencies. I can imagine a cartel-backed cyber currency where the values pegged and more stable because the cartel would control it and because you are talking about encrypted data and no physical manifestation that you have to exchange or move across borders. Do you think cyber currencies will eventually make this less of an attractive method of moving large amounts of money internationally?

Mr. Williams:
I am uniquely qualified to address Bitcoin with you and I think they are decentralized currencies. I think that there is a real issue with virtual currency as you saw in the recent Bitcoin up and down.

Mr. Cobb:
That's why I mentioned the cartel back. The Sinaloa Cartel controlled the algorithms and pegged the value and we dealt with them and they moved money and this is all done Silk Road style through shadow routers and it's not normal currency. Hypothetically, that type of system could be constructed, couldn't it?

Mr. Williams:
Yes, sir, it could in theory. It would be much easier – one is the ATM inventory require a piece of plastic. There is still a common thread that has to get it to a piece of plastic. Thus, you have to have a virtual account tied to this piece of plastic. I think that the virtual currencies are getting a lot of focus at this point. As a general rule, the anonymity of cyber funds will be offset by them being scared, even the cartels would be worried about a currency that went from $1,200 to a Bitcoin to $363 to a Bitcoin.

Mr. Cobb:
The reason I bring it up is an interesting aspect of the whole trend toward cyber currencies is there is a lot of data trail left behind that.

Assemblyman Anderson:
I appreciate your bringing up the virtual money. That's certainly something that we see in the technology realm.

My other question is what the lifespan of these cards is when you show us that they swipe into a hotel card versus getting it back onto some sort of spendable currency method. Is there a lifespan that these things go through that they have to hurry and do it within a certain time frame. Also, if you could speak to what the EU has done to their credit cards. I don't know if that is our FID technology or whatever is built into that versus having the mag stripe on the back.

Mr. Williams:
The timeline is really set by processor of the card so I could put a 10 year expiry on a card. When the card is manufactured, the expiration date is imbedded in the mag stripe as part of the information so there really is no timeline. As a general rule, banks replace them every two or three years because they pretty well get worn out. There really is no required time so they could build a card for 10 years.

There was much to do about nothing on mobile phones as a point of sale payment methodology. The reality is that it doesn't really exist today. There are rumors that there was going to be IPhone 6 that would have a chip in it. I don't think that's going to come to pass. There's a tremendous amount of disagreement within the two big constituencies in mobile phones. One is the networks – MasterCard, Visas, AmEx's, and the other, the carriers – the AT&Ts, the Sprints and the Verizons and where that information is going to reside. Why that's such a big issue is that taking an anonymous phone off of a shelf and walking up and saying – here's your new phone – and being able to put the magnetic stripe data that's on your plastic card and imbed it into an anonymous chip has become a nightmare for the industry. It's a significant issue. I think that's why today, you don't see mobile phone payments.

Mr. Anderson:
There are other technologies that are coming around once where you have a card that you actually swipe all your cards into and it stores that information and then you can use that one card as all of the others combined. Do you see those as becoming used in the same fashion or will that exponentially expand the opportunity for the criminals to use multiple cards into a single card? Where do you see that going as far as the security level?

Mr. Williams:
The rules and regs of MasterCard and Visa today say it's illegal to skim a card or to replicate the mag stripe on a device that was not produced in one of their approved and certified facilities. I will say the banks will fight to the death to prevent you from being able to consolidate your cards.

General Masto:
You were here about four or five years ago with you on some legislation to give our law enforcement the tools they need to really focus on some of these prepaid cards and identify whether there is money laundering going on or the currency there. Suggestions where we need to go next as a state particularly with any legislation that would be necessary to enforce or give our law enforcement the tools they need to address what you've just talked about today.

Mr. Williams:
I want to be very clear on the front end. I do have an agenda that I built this so with that said, I think that SB 82 combined with your seizure laws that are already in place, you have the ability today to be able to begin seizing cards, in my opinion. If found during an arrest or probable cause.

General Masto;
Thank you. I must say that this was a collective effort by this board, the Tech Crime Advisory Board that really was seriously looking into this and how we address this issue. Thank you, again, for coming back and presenting and working with the State of Nevada. We really appreciate everything that you've done.

Agenda Item 6 – Reports regarding Task Force and Board member agency activities.
No reports in the south or north.

Agenda Item 7 – Report from Executive Director.

Brett Kandt:
Once again, this is our first meeting since I took over as Executive Director and during that time, I've tried to reach out to all the Board members individually to discuss the Tech Crime Advisory Board, maybe perhaps reassess and realign its mission. Several topics have come up in my conversations with all of you.
1) The problem of data. When I talk about data, I mean statistics on the level of the problem we're encountering, the prevalence of tech crime. I think we all recognize the traditional crime categories in our uniform crime reporting look at violent crimes and property crimes, they don't adequately account for or track the rise of tech crime. That is something that has been brought back to me, I don't pretend to have an answer to that but I know it's something we will have to discuss moving forward.
2) The second piece has been the collaboration piece. I think we all agree, we don't need a state statutory board to collaborate. We are already doing that whether at the law enforcement agencies collaborating on the federal, state and local level or whether it be the collaboration between the public and private sector to minimize the opportunities for crimes facilitated through technology and to protect consumers.

Nevertheless, I am going to circle back to that collaboration piece towards the end of my report. In terms of our Board procedurally, three of the former members of the Board have left due to their terms being up or for other reasons. Undersheriff Balaam has left the Board because he was appointed by the governor to the P.O.S.T. Commission and under Nevada law, you cannot serve on more than one board pursuant to an appointment by the governor. U.S. Attorney Bogden's term is up and he is off the board now. With regard to Special Agent in Charge, Richard Shields, from the U.S. Secret Service, he has retired. I am meeting with the Special Agent in Charge for the F.B.I. here, in Nevada and with the new Special Agent in Charge for the Secret Service in Nevada in Las Vegas on Monday. I will talk to them about our Board and our efforts and how we can better collaborate and move forward together.

Moving on to federal legislation, obviously, there is an ongoing dialogue about possible revisions or amendments to Federal Electronic Communication Privacy Act or ECPA, especially the requirements with regard to what is required for law enforcement to access different types of electronic communications. That dialogue still takes place in Washington, DC. There's a new bill that's been introduced, actually identical bills in both the House and Senate, Senate Bill 1897, and the identical bill in the House, House Resolution 3990, entitled The Personal Data Privacy and Security Act of 2014 defines personally identifiable information and the act would do two primary things: 1) it would enhance the punishment for identity theft and other violations of data privacy and security. Specifically, it would amend the federal criminal code to make fraud in connection with the unauthorized act to access of PII, a predicate for instituting a prosecution for racketeering. 2) Second piece of this proposed federal legislation would subject a business entity engaging in interstate commerce that involves collecting, assessing, transmitting, using, storing, or disposing of sensitive information as defined in the act in electronic or digital form that involves 10,000 or more U.S. persons would subject them to requirements for data privacy and security that set forth in the act itself.

I think they are looking at those large scale data breaches that took place with regard to Target and some other entities and they are trying to insure there are greater privacy protections in place and notifications to consumers when there are such data breaches. Those are some developments in terms of legislation on the federal level.

I had also sent out to everyone today an email just to advise you if you didn't already know that on February 12th, the U.S Department of Commerce's National Institute of Standards and Technology issued a new framework for improving critical infrastructure cyber security that is a management tool that is designed to enable organizations to improve the security of their critical infrastructure. It is a product of a yearlong collaboration involving more than 3,000 stakeholders in the public and private sectors.

Two days later, on February 14th, they issued a roadmap for improving critical infrastructure cyber security which is a companion piece to that framework. It identifies key areas for cyber security development, alignment and collaboration including the development of better identity and authentication technologies, automated indicator

sharing, conformity assessments, data analytics and cyber security workforce. I emailed the links to the websites to those materials that provide both the framework and the roadmap that were developed. If anyone has any questions, please let me know. I think our private sector partners will be very interested in that.

Next, this year there are going to be a couple of very important cases at the U.S. Supreme Court looking at the issue of searching a cell phone incident during a lawful arrest. The first and probably the most important is *Riley v California.* There the court will decide whether the Fourth Amendment permits a warrantless search of the contents, including photos and video, of a smart phone seized during an incident to a lawful arrest. In this instance, Riley's smart phone was seized during an arrest and the police performed two separate warrantless searches.

They scrolled through the phone's contents at the scene, basically noticed some text messages and contacts that gave them reasonable suspicion to believe that Riley was involved in a particular street gang. Two hours later, after they conducted an interrogation to which Riley was unresponsive, they conducted a more thorough search of the phone. On the second search, they found more evidence and photos and video that indicated that Riley was a member of a particular gang. He was pictured with a car that police had suspicion had been in used in a prior shooting and basically, this led to charges that Riley was in the occupied vehicle involved in a shooting and charges for attempted murder, assault with semi-automatic firearm. Prior to the trial, Riley moved to suppress and that was denied. He was convicted. While the case was proceeding at trial, the California Supreme Court decided in *People v. Diaz* in which was held that the Fourth Amendment search incident to arrest doctrine permits police to search a cell phone, even sometime later at the stationhouse whenever a phone is immediately associated with arrestee's person. The California Court of Appeals affirmed his conviction. The California Supreme Court denied review so that is now up before the U.S. Supreme Court.

I won't go through the details of the second case, it's not probably as broad, it's a similar case in details but it involves an old fashioned flip phone and a narrower search of that phone that led to evidence that resulted in another individual's conviction.

We'll follow those two cases that the Supreme Court granted review and we'll look for those opinions later this year.

Finally, we've got a report coming up next on the agenda of the Technical Privacy Subcommittee. The subcommittee has done a lot of work. They have already met twice in December and February and have another meeting scheduled for April.

Last, in circling back to the issue of collaboration, this is a dialogue that's going on at the national level, it's obvious, that with the rise of tech crime, the current capacity, not only at the federal level but at the state and local level, to adequately investigate and prosecute technological crimes is just not there. Even though an important step was taken five or six years ago with the collaboration of the U.S. Secret Service, the National

Computer Forensic Institute was established in Alabama. That facility has actually had its funding almost doubled this year to train more investigators, forensic examiners and prosecutors but it just doesn't have the capacity to address the need. The NCFI can only, even in an accelerated training schedule that's now put in place, train maybe 2,000 people a year. That is not adequate to address the situation when we have over 40,000 state and local prosecutors nationwide, hundreds of thousands of law enforcement officers and our federal partners recognize they can't just take every tech crime case that comes up.

We've got to build up the capacity at the state and local levels to handle these types of cases. Because of that, I recently met with the Deputy Director of the U.S. Secret Service, A.T. Smith in Washington, DC, and discussed an idea with him that was well received about how we can build up the capacity on the state and local level without resorting to more brick and mortar training facilities. It's based upon a model that was utilized that began about a decade ago through myself and my counterparts in other states to increase or improve our ability to successfully prosecute traffic safety cases, and DUI cases. That model consists of placing specialized prosecutors in each of the states. Each state has one that specializes in traffic safety types of cases, impaired driving cases, and they work with the state and local partners to develop best practices and to train everyone to build up their capacity to handle those cases. It's been a successful model and I think it's a model that could be successfully replicated with regard to tech crime.

The goal is to place a tech crime resource prosecutor in every state that works closely with our federal counterparts and builds up that expertise and that capacity with the state and local authorities to investigate and prosecute these types of cases. I pitched that idea once again to Deputy Director Smith in Washington, DC, last month. The Secret Service is very interested in this because it's a model that has been utilized successfully before and they began discussing it with other federal partners including the FBI.

I was told today that it was taken to DHS Deputy Assistant Secretary Bill Flynn who is very, very receptive to the idea. I think, ideally, what they will do is a pilot project, just pick perhaps a dozen states to place initial tech crime resource prosecutors in to maybe work on somewhat of a regional basis with several states and eventually, once again, when we can demonstrate that this is a successful model and means to build up state and local capacity, they'll increase the funding for it and broaden it with the ultimate goal of having a tech crime resource prosecutor serving state and local authorities in every state. My goal is that Nevada be one of those first half dozen states to receive one of these positions on a pilot basis. I just wanted to keep you apprised of that I am going to continue to pursue this and my goal is that our federal partners here in Nevada would be integral to that effort to reach out with training and best practices to build up our capacity.

Agenda Item 8 – Report from Technical Privacy Subcommittee.

Mr. Kandt:
Hal Berghel is not here today. He is chairing that subcommittee but was not available for this meeting today. He did submit a brief status report that under Agenda Item 8 tab materials and rather than just recite that report verbatim, I am going to briefly review some of the different topics, how the subcommittee approached its efforts and what they have proceeded through up to date. We have another meeting scheduled for April. We are trying to meet every other month and the subcommittee has been very busy.

They started out discussing what latitude the states might have to expand constitutional privacy protections. It was noted that the Nevada Constitution in its Declaration of Rights, does not explicitly recognize the right to privacy, compared to the California Constitution which actually does expressly provide for a constitutional right to privacy. It was discussed 1) that's it's not easy to amend the Nevada Constitution; and, 2) even if you have an express right to privacy in a constitution as opposed to an implied right, it is still subject to delineation by the courts. Instead, the committee began to focus its efforts on 1) looking at the Nevada Revised Statutes and perhaps in some way, identifying those statutes that affect privacy rights and more specifically, digital privacy rights. Then developing a proposed strategic framework for improving those privacy rights, maybe, in part, predicated on the notion of disclosure and transparency.

The Subcommittee is reaching out to the Electronic Frontier Foundation for assistance because they have subject matter expertise and operate on a national level. They have assisted states in developing appropriate legislation to expand digital privacy rights. There were some specific areas that the areas that the Committee has begun to tackle. First, The News Shield Privilege under NRS 49.275 and whether that news shield privilege needs to be expanded to account for technology and third party records in the possession of free lancers and bloggers and other types of information that is not directly related to reporting itself.

Second, another area that the Subcommittee is looking at is possible amendments to NRS 205.473 through .513, that's the unlawful acts regarding computers and information services. The criminal penalties and the fact that those provisions were enacted over a decade ago probably need to be carefully reviewed and updated to account for changes in technology.

Dennis Cobb has looked at possible revisions to the State of Nevada's Online Privacy Policy.

Mr. Cobb:
We are going to refine it and continue to work on it but basically, we tried to come up with a framework that allows expedited and confident exchange of information between private and governmental entities. With no classification scheme for how important

information is, there's no way for me to know how you will treat it once you receive it. With prior agreement, we can say this is Level 1 that only requires a locked office door versus a locked file cabinet type of thing. It will facilitate that if Jim Owens wants to share something with Henderson PD, he can tell them that this is Level 1 and you can secure that properly. It facilitates a lot of things that now are just taken for granted. I think there are a lot of assumptions that how important I think something is how you will perceive it as well. We'd like to make that easier and more transparent for organizations and individuals.

Mr. Kandt:
Just a couple of other areas that the Subcommittee is looking at – possible expansion of the state's encryption statute which is NRS 603A.215. Talking about possible legislation to prohibit an internet service provider from lowering the level of security or privacy they provide without explicit customer notification.

Once again, some of these proposals are predicated on the notion of transparency or better disclosure. Discussion of possible legislation that prohibit the sale of security or privacy software that has been hobbled to lower protections below those that were advertised; possible legislation to prohibit the sale of software that has either security limitations or back doors without a complete disclosure; and, we are also going to look at license plate reader technology. I think that at some time in the future, the Committee will have some specific proposals for legislation that they will be bringing back to the Tech Crime Advisory Board for your review and consideration.

General Masto:
Thank you, Brett, and thank you to the members of the Subcommittee – you have been very busy with the important work you are doing and we all look forward to whatever recommendations that you bring before this board on the work that you are doing. Thank you.

Agenda Item 9 – Discussion and possible action on two proposals for legislation for 78th Nevada Legislative Session.

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

General Masto:
You have attached to your Agenda, a copy of the proposed legislation.

Mr. Kandt:
By way of brief background, last year there was a US Supreme Court case, *Missouri v McNeely*, and the details of the case aren't as important having to do with DUI arrests and the ability to forcibly require someone to submit to a blood draw to determine whether they exceeded the per se amounts under the law for legal intoxication while driving. During that time, the difficulty that our law enforcement agencies sometimes have in obtaining a warrant in a timely manner was brought to bear. It was also pointed

out that in many jurisdictions the technology exists and is authorized under their search warrant statutes that allows the officer in the squad car to dial in their probable cause affidavit via secure electronic communication directly to the judge who then turns around and issues a search warrant. It is a transaction that can happen in a matter of seconds. Our search warrant statute doesn't allow for that type of technology. This would simply allow for the technology. I developed this in consultation with other prosecutors who are supportive of it. I took it to the Nevada Sheriffs and Chiefs Association who certainly were supportive of it. I even reached out to the ALCU this week and they thought it was completely reasonable. I've had some judges review who are close friends of mine and who thought it was worthy of consideration and would be helpful so I've actually gone through the proper channels with the Administrative Office of the Courts to determine whether there is broad support among the judiciary for this proposal.

I wanted to bring it to your attention once again this is the piece that deals with allowing our law enforcement agencies to utilize technology to better protect the public. I welcome your feedback and ultimately, I would like to reach out at some point after I hear back from the judiciary to defense bar and ideally, I'd like to bring something like this to the Legislature that has broad support among everyone in the criminal justice community.

General Masto:
Comments from Board Members on this particular legislation?

Senator Ford:
I appreciate the concept and I think you are going about it the right way in terms of trying to get the broad level of support. I would also suggest that you coordinate with the minority interest organizations such as the NAACP and other sorts of organizations like that as well in addition to the defense bar so that you can get as broad a level of support as you can. It makes it a lot easier to make it through legislature when you have that kind of support.

Mr. Kandt:
Thank you, Senator Ford, I will most definitely do that.

General Masto:
Anything else you need from us. At least, from my perspective, I agree with the Senator that you are moving in the right direction by talking with all the broad stakeholders about this particular legislation. The only other question I have for you is who would be carrying the bill, would that be something that you would want ultimately, this Board to vote in support of and then be looking for somebody to carry it?

Mr. Kandt:
It's a question as to whether this Board is comfortable taking a position. This is listed as an action item so to the extent the Board is supportive of this proposal, even if it's just in concept, that's fine. If you want me to continue it as an agenda item for a later meeting,

after I continue to reach out to all the stakeholders and report back to you, certainly that's fine as well. In terms of who would carry it, I haven't identified anybody specifically yet. There are several possible avenues.

Mr. Cobb:
I just wanted to ask if it wouldn't matter, it probably isn't necessary for the statute about search warrants but due to the nature of the Board, I wonder if there is some place to put in requirements or recommendations or best practices regarding the medium of transfer of the detailed information in the affidavit and the encryption requirements. Because of the PII aspects of it and our role, maybe we could at least encourage that whatever agencies do this, I think it's a great law the way its proposed with the caveat that the information is protected to a reasonable level.

Mr. Kandt:
Certainly, the issue of protecting PII is a valid one. Currently, the search warrant statute doesn't address that issue, it's just a general, broad enabling statute that authorizes the issuance of warrants under certain situations and now, it just doesn't account for technology. It was amended at one point in time to allow for telephonic warrants so it was updated to that extent but it doesn't allow for other forms of secure electronic communications.

General Masto:
Would that be something that the Technical Privacy Subcommittee would take a look at potentially, to give some input to Brett on that particular legislation?

Mr. Cobb:
I think we could and I think probably just an inlet level of security is all we are talking about.

General Masto:
Any other comments? Is there a pleasure of a Board member or how we want to move forward with this legislation at this point?

Mr. Owens:
I think it's a great idea. I would just hesitate to slow this process down. I would be happy to move forward and contact these other sources for their input on it but don't slow down. I would move that we support this and keep it moving in this direction.

Senator Ford:
While the concept sounds good, I'm not comfortable at this junction being able to provide support for it without knowing about the input from the other organizations that we've mentioned including the defense bar, NAACP, MALDEF and other organizations. I think he just made a motion and if that's the case, then this is simply a discussion point, I will have to vote against the motion. That's my thought on this and that would be my preference.

General Masto:
We have a motion pending, is there a second to the motion?

Mr. Cobb:
I would second the motion.

General Masto:
We have a motion to approve this particular legislation and with the comments that were made, that Brett continue talk with stakeholders, gather more information and still come back to the Board?

Mr. Owens:
We do want him to continue and the support of these other groups but we don't need to wait for another one of these meetings to have him start doing that. My motion is to move forward as he explained and still obtain the consensus of the other interested parties but we need to go forward.

General Masto:
Any further discussion?

Mr. Anderson:
I would certainly ask the good Senator to, if we understand the process going forth, that we are not committing necessarily to anything that certainly would be a lot of time for discussion and open end opinions as far as the other stakeholders. Is there a specific time frame that would affect your opinion on moving forward on this particular agenda item?

Mr. Ford:
Let me clarify my point here – I don't mind moving forward with gathering information. I think that's certainly an important component of ultimately moving toward trying to get this submitted into a BDR and becoming legislation. My understanding of what we're voting on though is we support this concept that is listed on the agenda and I to reserve judgment on that because I don't know what the other stakeholders feel about it. So, it seems to me that the prudent thing to do is to wait until we hear from other sides relative to what the concerns and issues are because there may be an opportunity for us to support this in an amended fashion or maybe we support it if everyone comes back and says it's good in terms of the concept as it stands. I'm just not, at this juncture, in a position to be able to support the entire thing without hearing more information on what other stakeholders have to say about it.

General Masto:
Any further comment?

Mr. Kandt:

I just wanted clarification. I know that Senator Ford asked me to reach out specifically to the NAACP. As I indicated, I have already reached out to law enforcement, prosecutors, the ACLU, and all have been supportive. I intend to seek support from the judiciary and then the defense bar. Is there anybody else that I am missing in terms of potential stakeholders that I should affirmatively reach out to with this proposal?

Mr. Ford:
If you can think of any other minority based organizations that work in this area, I would suggest that you contact them as well.

General Masto:
Thank you, Senator. We have also a request for a clarification of the motion, Mr. Owens. So can you clarify for us, is your motion to vote not only on the concept but also to have Brett continue moving forward with his discussions with various groups on the concept and then to come back to this Board to give us an update or is it just a motion to approve the concept?

Mr. Owens:
I totally support Brett continuing this but this is not that complicated of an issue. This is simply technology taking the next step. We move from having to present a written document to the judge to be able to telephonic, this is just the next step in doing this. I don't know exactly what the problems would be. My motion would be to move forward, you can do a BDR but this won't go to legislature for a while if we determine if there are problems in the future that we address that long before we get to the legislature. I would move forward as it is written.

General Masto:
Any further discussion?

Mr. Cobb:
I just wanted to add that that was what I seconded was the concept of a different medium of transmittal of information. It's already gathered and moved to the judiciary every day by law enforcement. It will just be transmitted in a different way, is my understanding. That's what I seconded.

General Masto:
We've heard the motion. All those in favor, signify by saying "I".
Those opposed, "Nay".

All voted in favor except Senator Ford; one nay.

General Masto:
We voted and the motion has been approved. Brett, can we ask that as you move through this process, after you've talked with some folks, bring back and update the Board with respect to this particular legislation and what you are uncovering as well.

Mr. Kandt: Of course.

B. Amending NRS 179.460 to create and exception for the interception ("bugging") of oral communications in hostage and barricade situations.

Mr. Kandt:
By way of background, this is another area in which law enforcement has had concerns about the current statute – the way it's written, the way it reads, and the way it's been applied. In those situations where and we've got some law enforcement folks here that could probably describe this situation better than I because they have been in them. When you have a hostage or a barricade situation and law enforcement already goes through the process of seeking and obtaining the appropriate authorization under the statute to listen in to what's going on in that situation, a house, for instance. Seconds count in those situations and when they are going through that process, they have concerns about their inability that they are working without knowing what's going on in there, where if they had the ability to bug, they might have a better idea of what's going on inside, the situation, whether there's anybody at risk, whether the individual that created the situation that took the hostages or is barricaded in there might be about to take some sort of action that would require a tactical response.

I know that the Attorney General has opined informally that in those situations there is no reasonable level of expectation of privacy and therefore, it wouldn't preclude a bugging but the statute doesn't necessarily expressly allow that and so there has been some discussion about whether the statute should be amended. I don't have any specific language to propose to you but I just wanted to keep it on your radar.

General Masto:
You are not asking us to do anything now other than updating us on the potential issue and what may be moving through future legislation by either what this Board or somebody else says looking at this issue.

Mr. Kandt:
I'm working with law enforcement and the District Attorney's Office in Clark County closely on this. To the extent that there is some specific language proposed to amend the statute to address this type situation, I'll bring it to your attention.

General Masto:
Any comments?

Mr. Owens
For Las Vegas Metro, we are very supportive of this language. It's something we deal with on if not a daily, a weekly basis and I appreciate your help with this.

Agenda Item 10 – Committee Comments.

General Masto:

This is an opportunity for member of the Committee to address the Committee on any additional issues.

Mr. Cobb:
I just wondered if the Committee would be interested in maybe asking Jim Owens to give us his impressions. I have had people contact me about the new policy down south that they are not responding to traffic accidents and they have some concerns about the sharing of personal identifiable information and they don't really know what they have to give or whether they are at risk of someone impersonating them or committing some sort of fraud. Jim has a lot of expertise in both sides of this – the traffic and the detective end of it. I would be interested in whether he thinks it's an issue at all, whether there are guidelines, maybe the AG's office, that would be a best practices kind of thing. Agencies with limited resources have to look at this kind of process.

General Masto:
Correct me if I am wrong, I don't know if our General Counsel is there but I believe we would have to identify that as a future agenda item so that we are keeping within the Open Meeting Law.

Mr. Kandt:
I double as your General Counsel and yes, I would advise that we include that as a future agenda item that would be the prudent thing to do.

General Masto:
OK, we will add that as a future agenda item.

Mr. Cobb:
If Jim Owens isn't the right person to do it, he might be able to suggest someone. I know NHP has a lot of expertise in the area and the forms are state forms so maybe NHP would have better info, too.

Mr. Kandt:
Dennis, could you email me specifically just so we have the appropriate, concise language of what the agenda item is and what will be considered. Please email me what you'd like to see on the agenda so we get it right.

Mr. Cobb:
As soon as Jim tells me what he's willing to do, I'll write that down and send it to you.

General Masto:
Any other Committee comments? Hearing none, we'll move on to Agenda Item 11.

Agenda Item 11 – Date, Time and Location of Next Meeting.

General Masto:

I would recommend we allow Mr. Kandt to continue to help us identify that date and time. Are you ok with that?

Mr. Kandt:
In the transition from Belinda to myself, she had indicated that she had tried to put the Tech Crime Board on a quarterly meeting schedule. Looking at the first Thursday of the month, every three months which would be the first Thursday in June and then the first Thursday in September. Is that amenable to the Board? Do you want more flexibility than that and have me simply have my assistant contact you and identify a mutually convenient date? I'll follow whatever the Board's pleasure is.

General Masto:
The existing timeframe that we set seems to work for everyone unless you have an objection to that, speak up, or we will continue on the same path. I don't hear an objection so we'll just continue the way we've been operating.

Agenda Item 12 – Discussion and possible action on future agenda items.

General Masto:
We have one recommended already. Any ideas at this point in time, you are always free to provide before the next meeting if you have ideas. Send any ideas to Brett Kandt and he can add that to the agenda.

Agenda Item 13 – Public Comment.

General Masto:
There is no one here is Las Vegas; is there anyone in Northern Nevada that would like to address the Board at this time?
Seeing, hearing none, we will move to the next agenda item.

Agenda Item 14 – Adjournment.

General Masto;
Adjourned.

……