Minutes of the
Nevada Technological Crime Advisory Board

March 28, 2008

The Nevada Technological Crime Advisory Board was called to order at 10:00 a.m. on Friday, March 28, 2008. Attorney General Catherine Cortez Masto, Chairman, presided in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in Room 3138 of the Legislative Building, Carson City, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Special Agent William Bergin *(Designated representative for Resident Agent In Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE))*
Gregory Brower, U.S. Attorney, Department of Justice (DOJ)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Sheriff Mike Haley, Washoe County Sheriff's Office
Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)
Dale Norton, Nye County School District Assistant Superintendent
Nevada State Assemblywoman Peggy Pierce
Mr. William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Nevada State Senator Valerie Wiener
Mr. Tom Wolf *(Designated representative for Dan Stockwell, Director of the Nevada Department of Information Technology)*

Also present: *Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)*

TASK FORCE MEMBERS PRESENT:

Sergeant Troy Barrett, LVMPD / Internet Crimes Against Children
Supervisory Special Agent Eric Vandersteldt, FBI

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director
Conrad Hafen, Nevada Chief Deputy Attorney General, Advisory Board Counsel
Jill Mitchell, Program Specialist, Nevada Attorney General's Office
Ursula Sindlinger, Board Secretary

OTHERS PRESENT:

Dennis Carry, Washoe County Sheriff's Office
Janice Jones, ICE
Ira Victor, Infragard

Agenda Item 1 – Verification of quorum

AG CORTEZ MASTO:
We have new members here today as well as reappointments of previous members. We have a reappointment for Bill Uffelman who has been a tremendous help on this advisory board and we look forward to working with him. Tray Abney from the Reno/Sparks Chamber of Commerce has been appointed by the Governor. From our law enforcement sector we have Sheriff Doug Gillespie in Las Vegas and Sheriff Mike Haley from Washoe County. From the education sector we have Dale Norton, who is with the Nye County School District.

At the Federal level we have Special Agent in Charge Steve Martinez of the Federal Bureau of Investigations (FBI) who has served on this advisory board for awhile and has been reappointed. We also have Resident Agent in Charge Greg White with the United States Immigration and Customs Enforcement (ICE).

MR. EARL:
RAC White could not be here today due to some weapons training that he was unable to reschedule. He has designated a replacement who has not yet arrived.

AG CORTEZ MASTO:
Thank you. We have new appointees Greg Brower, the new United States Attorney from the Department of Justice, joining us well as Special Agent in Charge Richard Shields who is with the United States Secret Service.

A roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Welcome to new members.

AG CORTEZ MASTO:
Thank you. I welcome all of the Advisory Board members and we all look forward to working with you this coming year.

Agenda Item 3 – Discussion and approval of minutes from December 14, 2007 Advisory Board Meeting. Explanation of minutes production process.

Motion to approve the minutes was made by Sheriff Doug Gillespie and seconded by Bill Uffelman.

Motion to approve minutes passed unanimously.

AG CORTEZ MASTO:
Are there further discussions under this Agenda Item?

MR. EARL:
Madame Chair, I ask for a minute to explain, particularly to the new Advisory Board, how we try to deal with the minutes.

We have found, over the last Legislative session, that having precise and near verbatim minutes is really an asset when we are responding to questions from the Legislature. It is our objective to make those near verbatim quality minutes available to Advisory Board members within about seven to ten days after a meeting so that you can review them while the meeting itself remains fresh in your minds.

We would like to get corrections from you within 14 days which is a bit of a change from the distributing email that was recently sent out. After 30 days, the time required by the Nevada Open Meeting Law for minutes to be available to the public, we would like to continue to have them available to the public via the website. Thereafter any use of the minutes in the newsletter would

be appropriate. If that meets with the approval of the Advisory Board, that is how we will continue to work with the minutes.

Agenda Item 4 – Report regarding Northern Task Force Activities.

AG CORTEZ MASTO:
Mr. Earl, because we have new Advisory Board members here today, would you please explain how we handle Agenda Item 4 and 5 before we proceed with the reports?

MR. EARL:
These particular Agenda Items have existed traditionally and are divided in presentation by the North and the South regions of the State. It may be appropriate, given the fact that we now have additional agencies, some of which have activities in both the North and the South, in the future, to merge them into one Agenda Item.

Essentially this is an opportunity for any of the law enforcement agencies that participate in Task Force activities, or related prosecutions since we now have the U.S. Attorney as a member of the Advisory Board, to outline in a report what their activities are.

These reports provide other Advisory Board members with an opportunity to understand what is actually going on at a Task Force level and understand what investigative agencies are doing. At the same time it provides a record of activities that can be used to explain to Legislators during a Legislative session exactly what Task Forces are doing and how their mandates under the Statutes are being achieved.

However, it is really up to individual law enforcement agencies to report what they think is appropriate in the "tech crime" area.

These meetings are, of course, public so virtually all of the agencies are very careful not to disclose ongoing investigations. Even in those investigations which have closed, they need to be mindful that they are speaking to a public audience and not necessarily only to the audience that is here in the room.

AG CORTEZ MASTO:
Thank you. With respect to the report regarding the Northern Task Force activities, typically we would have a report from the representative from ICE in the north. At this juncture, I am not sure whether or not there is a representative who is prepared to talk about that.

We now have Sheriff Haley joining us. Sheriff, because you are new to the Advisory Board we would definitely understand if you would like to take a pass on this now and wait and see how we have traditionally discussed these items.

SHERIFF HALLEY:
I will take a pass on this for now. I did meet with the Director of this Advisory Board and we went through all of the policies, procedures and the new changes to the Nevada Revised Statutes. I met with members of my staff who are participating in various "tech crimes" activities and I am becoming more familiar with how that relates to this group.

AG CORTEZ MASTO:
Thank you. Let us move on then to Agenda Item 5.

Agenda Item 5 – Report regarding Southern Task Force Activities.

AG CORTEZ MASTO:
Let me mention someone I have here today who is a representative from my office. Greg Smith is the new Chief of Investigations and he will be working with the Task Forces both in the north and

in the south. We also have Conrad Hafen who is Chief of my Criminal Division and he is an active participant with us in discussions of this Advisory Board.

With respect to the Task Force in the south, are there any members who have any comments or reports to give at this time?

SA VANDERSTELDT:
I am Special Agent Eric Vandersteldt with the FBI and I have some comments I can make regarding this Agenda Item.

First of all, I would like to thank Mr. Jim Earl, Mr. Greg Smith and Ms. Jill Mitchell for paying our office a visit last week to see where we live and work. It was a very cordial visit and I appreciate that they took the time, especially the folks from up north, to come down to see us.

I would also like to introduce Sergeant Troy Barrett with Las Vegas Metropolitan Police Department (LVMPD) who is on the Internet Crimes Against Children Task Force (ICAC). They are co-located with us at the Southern Task Force here. Troy brings a number of excellent qualities with him to that position and I want to thank LVMPD for putting him in that capacity with us. We look forward to working with him.

Since the last Advisory Board meeting, we have had several cases that have culminated in indictments, arrests and convictions. Due to the same reasons Mr. Earl had mentioned earlier, I cannot go into pending investigations but I can point out a couple of cases here to give you an overview of the type we do work.

A subject who had posted and shared photos depicting child pornography utilizing a PhotoIsland account pled guilty and was sentenced to the mandatory minimum of five years in prison.

Another subject was charged with advertising child pornography under a Federal Statute pertaining to that issue, which carries a mandatory minimum sentence of 15 years in prison. To my knowledge this is one of the first times that we have used that statute here in the District of Nevada. It carries a very significant penalty and it is a very good tool for federal law enforcement.

Those are the only two cases I would like to mention at this point. Computer forensics have always been a topic in these agenda items and I would like to point out one area related to the this. During the period from the last meeting to this meeting we performed forensic analysis of data exceeding eight terabytes on more than two dozen cases. To put that into perspective in terms of how much data that is, one terabyte would hold about one billion business letters.

In conclusion, I would like to also thank everyone who was involved in the selection and the hiring of the computer forensic examiners that the State of Nevada hired into the Attorney General's Office. We have one working with us named Bill Capps, who is off to an excellent start. We really appreciate all the effort that went into his selection, hiring and placement with us.

That is all I have and now I will turn it over to Sergeant Barrett.

SERGEANT BARRETT:
I am Troy Barrett with ICAC Metro. Nothing specific but we have a few ongoing investigations with a couple of search warrants. Examinations have to be completed before we actually get approval for probable cause arrests. We have a trial coming up in two weeks which is another federal case. We are also going to start to do some more local charges instead of federal. Federal carries more weight in the way of prosecution and time served then local cases usually do, but we are getting ready to start a relationship with Jim Sweeten, who now is one of our new Team Chiefs, to see what we can do about charging people locally instead of just going federally.

AG MASTO:
Are there any questions from the Advisory Board? Hearing no additional questions, let me ask the gentlemen a quick question with respect to the Internet Crimes Against Children. I know during the last Legislative session, we passed some state laws allowing some undercover work with respect to those activities. Are there any other laws or other types of tools that you may need to carry out the functions of your office?

SERGEANT BARRETT:
Just recently the United States Department of Justice (US DOJ), who gives us funding each year for training and equipment, did a quality of review process and came down and made some good recommendations in the realm of undercover work. We cannot go into tactics, obviously, but we are going to be bringing an individual down who is an expert in this from Wyoming. He will come down and train each one of the four investigators that I have on my team and we will open it up to some of the affiliates that we have. Of course, those affiliates would be Washoe County, Elko County and our new affiliates of Henderson and Mesquite. I also have a couple of other affiliates who are waiting for Memorandums of Understanding to get signed by the Sheriff. Those affiliates are Sparks, Carson City and, I believe, the School District Police in Washoe County also.

We are in the realm of getting everything set legislative-wise. I cannot think of anything else off the top of my head. I am sure something will come up and I will definitely approach you at that time if we are in need of assistance.

AG MASTO:
Thank you, Sergeant Barrett. Are there any other members of the Southern Task Force who would like to speak at this time? Greg Smith, please go ahead and speak.

CHIEF INVESTIGATOR SMITH:
We recently filled our last computer forensic examiner position. He will start on April 21, 2008 and be located at the Secret Service office in Las Vegas. He comes with quite a bit of experience and we look forward to having him as the final member of our task force.

AG MASTO:
Thank you, Greg. Are there any other comments? Hearing none, we now move on to Agenda Item 6.

Agenda Item 6 – Overview of Infragard and activities of the Sierra Nevada Members Alliance (the Reno chapter of Infragard).

MR. IRA VICTOR:
Thank you, Madame Chair and members of the Advisory Board. My name is Ira Victor and I am President of the Sierra Nevada Chapter of the FBI Infragard which I will get to in a moment. First, I have just a little bit of business.

Mr. Tom Clark was going to be speaking to you today but I received an email from him on my way here. He is ill with the flu and has asked me to make some comments in his absence today which I will present to you from his email thanks to Blackberry.

For those of you who may not have heard of Infragard, I will give a brief introduction of our organization and how we might be able to help the Advisory Board.

Infragard is spelled I-N-F-R-A-G-A-R-D. The joke in the group is “the only thing missing is U”. Infragard is designed to protect the nation’s critical infrastructure. It is a program of the FBI. The feel of the FBI when Infragard was first started was whether it was drinking water supplies; communications systems; the Internet; the banking system; the chemical industry; the public health system; or the transportation systems, for example, all of these systems are critical to the

nation's health and securing those systems becomes important especially in a post 9-11 environment.

The federal government felt that since most of that critical infrastructure is run or controlled by the private sector that the government could not possibly protect it with only government resources. It needed to have a cooperative effort between the private sector and the public sector to protect these critical infrastructures.

The Infragard organization is based with each FBI office around the country. There are about 130 plus chapters nationwide with between 20,000 to 25,000 members. The number continues to grow. Members are private sector and public sector people who come together to facilitate communications about infrastructure security needs. We have also created a subject matter expert database. When there is a subject matter expert needed in a particular area, then the Infragard program can utilize members in that specific field of expertise for law enforcement members to call upon for help.

I can speak in detail as President of our chapter in northern Nevada. Generally, we meet in public every quarter although sometimes we have confidential meetings. Typically we host speakers and seminars to facilitate the communication between public and private sector on these critical infrastructure issues.

All of the members of Infragard have gone through an FBI background check process to make sure that we do not have any rotten apples in the satchel. As I stated, sometimes we do have confidential meetings that are not open to the public where more sensitive information is shared and discussed with the members.

There is an abundance of academic research that indicates that when people in the private sector communicate with members of law enforcement about threats, then law enforcement is able to tie together patterns and go after the bad guys.

For example, the private sector members may see something happen here in Reno that appears to be a certain type of attack or threat that may seem to be minor and insignificant. If we share that with our law enforcement partners in Infragard, they may be able to connect that behavior to something within their own databases and go after the bad guys.

One of the reasons I am here today is to offer the services of Infragard and our members to help the members of this Advisory Board. The issues out there are getting rather complex, especially the cyber crime and Internet issues. The technology changes very quickly. The types of attacks that the bad guys use are always changing. It is a challenge for everyone to stay one step ahead of the bad guys. It is especially a challenge for government, which has to go through its normal processes. Government may be a little bit slower than criminals or bad elements when it comes to maneuvering.

We want to offer our help and assistance today, and at any time, with issues that have to do with critical infrastructure and security. Of course, it could be as little as answering a short question in an email to something that is more in depth.

Although we have also some information about potential bills for the next Legislative session for review shortly, this invitation for assistance is extended to you anytime throughout the year.

Finally, I want to bring up an area of concern that we are following at Infragard that has to do with breach disclosures. It is a really growing issue. There are questions about when there is a breach and how it should be disclosed and what different details should be included. Without getting into the weeds of that today, I just want to bring up an example that was in the news recently.

A student at Harvard University became aware there was a lack of security surrounding student information. So, on his own, he hacked into the Harvard computer network and copied a lot of sensitive student information. He then redacted the Social Security Numbers and other information that bad guys could use and posted that redacted version on the Internet to send a message to the university of "wake up!"

This brings up a whole hornets nest of legal issues. This is an example of the type of activity that is going on out there: bad guys acting badly and good guys acting in a positive way and then people who seem to be good guys acting in a way that appears to be good. I do not want to get down into specifics of this example. I brought this up to highlight the complexity of the issues that we are all facing here and how Infragard can help the Advisory Board and answer questions about these complex issues.

Let me also share what types of members are involved in Infragard. We have an incredibly diverse type of membership. If anyone on the Advisory Board knows of anyone who might want to join Infragard, there is no cost to join. The FBI picks up the cost of their background records check.

We have members who are in law enforcement at the federal level such as the FBI but also from the County Sheriff's office and local police departments. We have someone from the Washoe County Fusion Center. Members come from the University of Nevada Reno academic community, the local power company, the water authority, the gaming community, the banking and financial services community, for example.

Think about critical infrastructure that has information that could be valuable for the bad guys to get their hands on to disrupt services and industry. Those are the types of people who are on our board and are members of our organization.

AG MASTO:
Thank you, Mr. Victor. Are there any more questions?

MR. ABNEY:
Thank you, this is Tray Abney. Our agenda mentions that Infragard has been the subject of inaccurate criticism in the blogosphere lately. Could you speak to that?

MR. VICTOR:
There was a story that appeared in a magazine. I do not know if it was a print magazine and a website magazine or website only. I do know it was not a "Time" magazine or one of the more traditional mainstream media sources. They did an interview with someone who claimed that they were a member of Infragard. A reporter quoted this person saying that Infragard members have the ability to "shoot to kill" or something really goofy. That may not have been a real Infragard member who was interviewed because we do not get into firearms at all. Firearms are not on our list. We are not issued firearms. Infragard has nothing to do with firearms.

So either that person was not in Infragard or that was a person who had been in Infragard who was making a sarcastic comment that was taken out of context. There has been a lot of chatter on the Internet about this with insinuations that somehow Infragard is some sort of "Skull and Bones" secret society and we are like "007" guys running around with "shoot to kill" licensed ability.

None of those stories or rumors are true at all. As President of the local Infragard Chapter, I can assure the Advisory Board of that.

AG MASTO:
Thank you, Mr. Victor. Are there any further questions or comments regarding this subject for Mr. Victor?

ASSEMBLYWOMAN PIERCE:
Just to be clear in my mind, we are talking about any kind of infrastructure here. We are not just talking about technological infrastructure?

MR. VICTOR:
That is correct. Let me read from Infragard material from the FBI. This is what the FBI classifies as critical infrastructure: agricultural and food; banking and finance; chemical; defense; industrial base; drinking water and waste water treatment systems; emergency services; energy; information technology (such as the cyberspace world); national monuments and icons; postal and shipping systems; public health and healthcare providers; telecommunications; and transportation systems.

So it addresses both physical security and cyber security around those industries. That was a very good question, Assemblywoman Pierce. Thank you.

AG MASTO:
Thank you, Mr. Victor. Are there any further questions or comments from Advisory Board members? Yes, Mr. Earl, please continue.

MR. EARL:
I have been to most of the Infragard meetings of the Reno Chapter since I have been associated with the Advisory Board. I think that Mr. Victor has downplayed both some of the activities that I have seen and his own leadership role in Infragard.

Typically, what happens in an Infragard meetings is that several of the Infragard Board members, and Ira is always one of them, will give about a 15 to 20 minute presentation on threats that have emerged over the last meeting period. Sometimes, these presentations are very explicit and make sense to folks with considerably more Information Technology (IT) background than I have. These presentations are designed to share Ira's and the Infragard Board's information with all of the public and private sector members in attendance. This allows everyone to be brought up to date with regards to ongoing threats.

In the Reno Chapter, Ira has managed to attract some outstanding speakers who we probably would not have the opportunity to hear from otherwise. My favorite speaker, of course, was Sheriff Haley who spent some time at one of the recent Infragard sessions explaining what he perceived as local threats in the northern Nevada area.

Another past presenter was the Central Intelligence Agency (CIA) Station Chief who was part of the first team into Afghanistan and was followed only afterwards by teams from Delta Force. He discussed some of his experience in Afghanistan and what he was able to read from that into what he perceived as potential threats directed against the United States today.

The last truly spectacular speaker that I heard was a gentleman who had his identity stolen while he was dying of cancer. The good news is that he became sufficiently upset about the whole thing and it probably kept him alive. Eventually, from his hospital bed, he tracked down the perpetrator who turned out to be employed at one of the specialty hospitals where he had been treated. The perpetrator had read this individual's medical records. He knew the patient was going to die and assumed his identity and committed a series of financial fraud crimes while the patient was still alive.

At the time, because of how sick this victim was, he had great difficulty attracting the attention of law enforcement to his predicament. He was finally successful and related the story to the Infragard Reno Chapter members. I have stayed in touch him and at some time in the future it may be appropriate to ask him to speak the Advisory Board if we can work it out with him to make the trip from Silicon Valley over the mountains to Carson City.

AG MASTO:
Thank you, Mr. Earl. Mr. Victor, thank you very much for your presentation.

Before we move on to the next agenda item, for the record I want to welcome SAC Steve Martinez from the FBI who has joined us and SAC Richard Shields from the US Secret Service who has also joined us down here in the south. Thank you.

MR. EARL:
Madame Chair, we also have just been joined by representatives from the Reno office of Immigrations and Customs Enforcement and will ask them to introduce themselves.

SA BERGIN:
Thank you, my name is Special Agent Bill Bergin with Immigrations and Customs Enforcement. Thank you for having me here today.

SPECIALIST JONES:
Hello, I am Janice Jones, Mission Support Specialist from the ICE office in Reno. Thank you for having me here also.

AG MASTO:
Great, thank you for joining us. Let us move to Agenda Item 7.

Agenda Item 7 – Presentation on capabilities of i2 software in support of local law enforcement.

AG MASTO:
Ms. Mitchell, who is one of our newly hired Attorney General's Office (AGO) tech crime positions as analyst, is going to be giving the presentation.

Let me just stop you before you get started. It is my understanding that we want to thank the FBI for assisting you with printing the maps on their plotters that you are going to be presenting to us today. Is that correct?

MS. MITCHELL:
That is correct. The FBI was gracious to loan us their plotter to print that out. I will be talking more in depth about that in just a little bit.

Good morning. I would like to thank everybody here for your time to allow me to come here and let you know what I have been up to since I was brought on staff in December. Some of you I have met previously at the last Advisory Board meeting and also, recently, on my trip down to Las Vegas. There are some of you whom I have not had the privilege of meeting.

As an introduction, my background is all law enforcement and I have been in the law enforcement community for about the last 17 to 18 years. I was a police officer in Nebraska which led me to the intelligence division of the Nebraska State Patrol for about seven or eight years as a crime analyst. Then I spent the last four years before I came here to Nevada as a trainer and a consultant for an investigative analysis software company based out of Washington D.C. called i2 Inc. That company produces the investigative analysis software that I am currently using.

One of my duties as an AGO analyst is to analyze the Internet Crime Complaint Center (IC3) reports that the Attorney General's office and other local law enforcement offices receive from the National White Collar Crime Center (NW3C), which is part of the FBI.

These are sent to us via email and we average anywhere between 150 to 200 reports a month. I have utilized the i2 analytical software to build a database of this information. I am populating this database with all of the information from these numerous reports.

I did bring some really quick statistics for you to date. As of today, I have about the last six months of data in the database which covers from August 2007 to February 2008. There are about 1,100 people in the database; 1,100 addresses; over 1,000 email addresses; 900 telephone numbers and over 200 website addresses.

Now, something to keep in mind is that this is just the IC3 data. This is not anything that is being received from the Federal Trade Commission (FTC). This is just the IC3 data.

I broke the IC3 data down a little bit by northern Nevada and southern Nevada as far as total losses. A ballpark figure for a total loss based on these reports from northern Nevada is about $340,000. and a ballpark total loss for southern Nevada, a much larger population area, is sitting at about $1.5 million.

I want to give you an idea about just how large this problem is. Using the investigative and analytical software package allows us to is look at all of these Internet crime reports as a whole, not just individually. When we look at them individually, we might not see any patterns and we might not see any commonalities. When we are able to look at everything as a whole we can really start to see the big picture. We can see how all of these websites and all of these email addresses and some of names are connected together. We can see the commonalities.

The i2 database application is called a relational database. It gives us the opportunity to see the commonalities such as to see that a particular address is connected to more than just one complaint. We can actually see that an email address has been received three or four times in three or four different complaints.

This tool provides us with an opportunity to see the bigger picture. It is also a way to identify problem areas a little bit faster.

Let us look at the chart that you have in front of you. What you are looking at is data that I actually pulled out of the database.

Now, I will tell you straight up that because this is a public meeting, all the pertinent data on that chart has been changed. I changed the names, the email addresses, the phone numbers and the addresses. However, what you can still see are the connections. All the lines and how everything is connected together actually do exist in this case.

Again, if you look at just each individual report, it doesn't really seem like a lot. Maybe you have a victim here who has lost $1,100. and another who lost $1,300. over here and another with $400. over there. When you start looking at those as a whole and bring those all together to see a bigger picture and start adding up all of those dollar values then that is a way to help identify a problem.

What is happening in the particular example case is fraud related to non-existent items. Perpetrators are posting false ads on the Internet. People are surfing around the Internet. They like an item and decide to purchase it. They may wire transfer the money or they may send a money order. Once the perpetrator has the money, they vanish and are never heard from or seen again. So you have all these different victims who are out of thousands and thousands of dollars.

Another thing of interest is that as you start going through all of these different kinds of reports, you can see that some of these perpetrators are actually using their real names, addresses, phone numbers and email addresses. We do have some things that we can look at from an investigative point of view to try and establish a case against some of them.

The sample chart was produced by the Investigative Analysis software package. I spent the last four years of my career as a trainer and a consultant for that particular software company and traveled all over the world to help different law enforcement and U.S. military installations with their data.

What is nice about the Attorney General's Office having this software application is that there are a lot of other law enforcement agencies within the State of Nevada using it. This makes it easy for us to share information. The FBI uses it. Las Vegas Metropolitan Police Department uses it. The Secret Service uses it. Reno Police Department uses it and the Nevada Department of Public Safety uses it.

I have currently established liaisons with a lot of the analysts with the FBI in the north and in the south and the Secret Service. I am working with Sheriff Haley to get in and meet with people at the Washoe County Fusion Center. I plan to visit the ICE office and the Secret Service in the north too.

Since these different law enforcement agencies use the same software package, I have agreed to use my software expertise to assist the other analysts and investigators using the software. This way we can develop a rapport with all of these agencies and start sharing all of this information to really work cases together.

Now for agencies without access to that software application, we can still share the information. Number one – we can print a case chart off into a pdf (portable document format) and send it off in an email. That agency can also download the i2 software reader that supports this application. It is called Chart Reader and it works very similar to Adobe Reader. It is a reader that can be downloaded for free from the Internet. Then we email them the charts and they have the ability to actually see the chart in electronic format. They can zoom in and zoom out. They can even print the chart off if they need to. Again, sharing the information is what we really want to do so we can work together.

Now, because of all of this and because I am relatively new in this position and I am just now starting to get out and get to know all of my counterparts, there may be a couple of things that all of you as Advisory Board members can help me out with.

I have limited access to some of the resources to try and identify some of these people, addresses, phone numbers and email addresses. This means the results are no better than the scope of the data that other analysts or I have access to.

I am asking some of you on Advisory Board if there might not be some things that you can do to help me gain access to some of the other resources that are out there to use. A couple of them that I am interested in would be the Financial Center (FinCen) database of the banking industry. This would allow us to search for Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs). Another database that would help would be belonging to the Nevada Department of Motor Vehicles.

Sheriff Haley, maybe you could help me out on this one. I do have access to your Tiburon system but only in a limited capacity. I cannot download the booking photos, and, if there is an additional report that is connected to one of the entries, I cannot view the report. Maybe that is something that you and I can work on together with your Lieutenant.

I do have some contacts at the Reno Police Department but I do not know if they have any type of "Intel" database. At this point, most of the people I have been dealing with over there right now are in the administrative sector. I am currently working with the FBI down south to try and get access to some of their resources. I think that will probably happen because I do currently hold a top secret clearance level from the FBI.

Another resource that I am interested in is called SCOPE which is the “Intel” database that I believe Las Vegas Metro uses. If there is anything that the Advisory Board members could do to help me out that would be wonderful.

Thinking long term, something that we could all do together is to someday convince NW3C and IC3 to provide the data in an electronic format instead of sending it in a Word document. That would speed up the process of getting the information into the database so that I can analyze it. At this point, they tell me that they just do not have the capabilities but down the line that will change.

Also, something else that we need to be thinking about it the data that I have given you on the chart sample is strictly from the IC3 information. That does not include any of the FTC information. The problem is that the FTC does not push their data out to law enforcement. Maybe that is something we need to look at a little bit further down the line.

SHERIFF HALEY:
I have a question. First of all, are you familiar with Zanalyst?

MS. MITCHELL:
Yes and no.

SHERIFF HALEY:
Then maybe you will not be able to answer my next question. We have that particular system because we are on a Tiburon database. I do not know if there is any connectivity or ability for our Tiburon database to be moved to i2 easily or can it be moved from Zanalyst to i2?

MS. MITCHELL:
That I do not know because I do not know how Zanalyst is set up on the back end. That is something that I would like to find out if that is possible.

SHERIFF HALEY:
What it would require is for us to have two of these analytical tools which are costly and the licenses are costly.

MS. MITCHELL:
I completely understand that. Maybe when I meet with your group at the Fusion Center, we can discuss that. Let us see if we can work that out.

SHERIFF HALEY:
Thank you.

MS. MITCHELL:
That is basically all I have to present to the Advisory Board today. If there are any questions, I can take those right now.

MS. JONES:
Hello, I am Janice Jones from the Reno ICE office. I imagine a lot of my questions could be answered if we could set up a time for you to come up to our office and meet everybody. Maybe we can exchange cards after the meeting today. I use the FinCen database and I can give you my contact. I think that is also the federal contact, but I do not know what the guidelines are for sharing that database. We can start by contacting them and see what we run into to get you access.

MS. MITCHELL:
That would be wonderful. I would appreciate that assistance. Let us definitely exchange cards.

MS. JONES:
Also, are you suggesting that other agencies purchase a license in order to access the i2 database to conduct our own searches? Or are you suggesting that we pose a request for search through the software company and then just read it? I am a little confused about what is being suggested.

MS. MITCHELL:
We are not at that level yet. I suggest that if you or any of your investigators are interested in the IC3 data I have compiled, please contact me. I can query the database for them. The database is not in a format yet to be shared and there would definitely be some financial costs to do so. For right now, it would be best if we would just work together. If you have a name or an email address that you want to check on then just give me a call and I will query what I have to see if that is in the database and then we could go from there.

AG MASTO:
Thank you. Are there any further questions from the Advisory Board members in the north for Ms. Mitchell? Alright, hearing none, are there any further questions from Advisory Board members in the south for Ms. Mitchell?

SAC MARTINEZ:
This is Steve Martinez from the FBI. I am really excited about the fact that Jim had the vision to get this ball rolling. In my former capacity as the Deputy Assistant Director over the FBI cyber division, which has the IC3 program, we were often asked by the United States Congress about what was happening with the referrals of this information that is getting kicked out there.

We had a very difficult time answering that question because there was not a good feedback loop. We knew a lot of good information was going out to state and local law enforcement nationwide and we did not often hear back.

This to me is a great step forward in starting, at least at a minimum, to get a better handle on what the crime problem is in some of these areas and then using that to start making decisions about resources and whether or not we can start to aggregate cases to meet certain thresholds for example.

The fact that we have gone down this road really starts to validate a lot of the time and effort that the FBI put in to get IC3 up and running with the support of Congress. I think we are much better off as full participants now here in Nevada.

Also, because I do have some contacts still set back there, I would like to offer an opportunity for you to get back to Washington D. C. You could sit down with the IC3 folks so that they can run you through the entire capabilities to give you a good handle on it. This is something that we can probably help facilitate. If you have a moment after you have your feet a little more wet, I think a trip up there would be a good opportunity for you.

MS. MITCHELL:
That would be great and thank you for the offer.

AG MASTO:
Thank you, SAC Martinez. Are there any other questions or comments from the Advisory Board members in the south? Hearing none, I also offer to Ms. Mitchell at this point, that if there is any information that you need from the State such as the Department of Motor Vehicles, you can work through our office. Several of my attorneys represent the various State agencies so we would be happy to work with you to get the information if it is available for your access. Thank you so much for your presentation, Ms. Mitchell.

MS. MITCHELL:

Thank you and thanks for your time.

AG MASTO:
Alright, we move on to Agenda Item 8.

Agenda Item 8 – Legislative Issues:

a. Statutory proposals responding to concerns initially identified by LVMPD.

MR. EARL:
As an update, at the last meeting there was a presentation by Sheriff Gillespie and several members of his staff and from that flowed a working group that was established with Attorney General Office personnel, some Lieutenants from Metro and me. We wanted to address some of the concerns that were identified during that presentation.

The first concern was the difficulty in obtaining information from Internet Service Providers (ISPs). The particular background paper containing statutory draft language remains a work in progress. However, our initial assessment is that the difficulty actually flows from the fact that the Nevada Statute dealing with how to obtain information from ISPs did not meet the federal test.

Essentially what has happened is we are into a problem of federal preemption where a national ISP such as AOL (America On Line) or Google or AT & T would receive a request where local law enforcement had complied with Nevada Statute, which required only a subpoena. Then their legal counsel looked at what was being offered from law enforcement in Nevada and looked at the federal law and found that it did not meet the standard established for State proceedings under federal law.

This paper (Attachment 8a) outlines that particular problem and represents our best attempt at this time to update the Nevada law but to do that in a way that is relatively intelligible to the individual law enforcement officer. Mostly small to medium sized law enforcement organizations in the State do not have immediate access to an attorney on their staff. We wanted the particular Nevada statutory language to be as readable as possible and, certainly, more readable than the governing federal law.

We have a request out to the Council of Prosecuting Attorneys to obtain some input from them as well. I would be glad to take questions or answers, but at this particular time, this does remain a work in progress.

The second piece of legislation that flowed in a similar manner was that Sheriff Gillespie and his staff indicated that they perceived a growing problem with criminals using electronically reconfigured hotel room keys. This occurs by replacing the electronic information on a magnetic strip with information which had been stolen from credit or debit cards that came from a variety of sources.

That led us to look at the statutory language dealing with debit and credit cards to ensure that it was broad enough to cover those instances where an actual credit card was not being used. In an attempt to bullet proof that particular problem there are some proposed changes that we continue to consider. These have been passed on also to the Council for Prosecuting Attorneys for their advice and input.

Another concern that was expressed and is also embodied in the second paper is about the length of sentences that was allowable for certain types of frauds. We did not address that across the board but we did look at the type of frauds that were described at the last meeting. Some of the penalties associated with fraudulent credit card use and forgeries associated with credit cards were increased. We wanted to address attempts to make or, in some other way, use information on a card that was derived from another source.

The third area that is not represented here by a separate piece of paper is that there was concern and an interest expressed in trying to look at a new Nevada statute which would be patterned on the gang statute. It would allow for an enhanced penalty if a perpetrator were found to use fraudulent materials and fraudulent credit cards as part of an overall scheme. At least to date, we have not been terribly successful in doing that and there are some good reasons for that.

With the increase in penalties that we are looking at proposing for credit card related frauds in general, the need for a penalty enhancement goes away. Moreover, statutes, such as the gang participation statute, typically read in such a way so that the enhanced penalty runs concurrently with the penalty that has been adjudicated for the underlying crime. So adding a comparable statute dealing with very loose affiliations in credit and meth rings might not increase actual penalties.

I think that is all I have with regards to Agenda Item 8a. If there any comments and suggestions, then great, but as I have said, we are still working on this.

AG MASTO:
Thank you. Are there any comments or questions from the Advisory Board members?

SENATOR WIENER:
Jim, as you are reviewing these issues and coming up with draft language, are these drafts for the Attorney General to bring forward as bills through her office or are these potential bills that you want us to carry as individual Legislators? As I ask this because some of these are issues that I have carried forward in the past.

AG MASTO:
Actually, I can say that we have not discussed that so I am amenable to any format on how you want to handle that, Senator Wiener.

SENATOR WIENER:
I am offering because I have carried similar bills. In fact, I shared with some children who I visited with in schools the other day about early involvement with identity theft related to the swipers and re-encoders. I carried some of the original legislation on that which included even having the possession of one of those would be the presumption of using the device to steal identification information off a credit card. So, I have worked this issue before and I am volunteering to move forward with this.

AG MASTO:
I would be happy to defer to you, Senator Wiener. Are there any other questions or comments from Advisory Board members?

MR. UFFELMAN:
Jim, are you comfortable with me sharing this document with VISA and others in the card industry to make sure there are no enhancements that they may want to add? Is this a work in progress or are you comfortable that you have finished the work?

MR. EARL:
It is a work in progress. This means that we have not locked it into stone. It is not close to a Bill Draft Resolution (BDR). We are still waiting for input from the Prosecuting Attorneys group. I have no difficulty with you sharing it with members of your organization and the broader banking community. I would be open to any suggestions that they think may be appropriate in light of their experience. It is perfectly possible that we have missed something or have drafted the new text in such a way so that it may cause some problems that we simply did not see. I think that would be a really good thing to do.

MR. UFFELMAN:
I will send it out to the Electronic Payments Coalition this afternoon.

AG MASTO:
Thank you. Are there any other further questions or comments on this subject? Hearing none we will move on to Agenda Item 8b and presenting this is Mr. Ira Victor or Mr. Tom Clark. Is that correct?

b. Issues related to the October 2008 entry into force of NRS 597.970 requiring Nevada businesses to use encryption when transferring personal information.

MR. VICTOR:
Or it may be Mr. Victor and Mr. Victor substituting for Mr. Tom Clark due to his illness. Thank you, Madame Chair.

First, as President of Infragard, I have been in communication with Mr. Clark and I work in the field of information security working for an information security consulting firm. So this particular cyber security area is one that I have a lot of expertise in, especially in encryption, which is hairball of an issue to understand.

When someone makes a claim that something is encrypted that does not necessarily mean that it is truly difficult to read. There is a lot of confusion about this topic. One of the community services that we are doing in Infragard next month on April 17th in Reno is that we are having an entire seminar with an encryption expert to just explain what it means when something is encrypted and when that term is appropriate to use. So if any of you want to know about that, I left my business card with the secretary. Please feel free to email me and I will send the information to any of you or anyone you make think may want to attend that meeting on April 17th.

Let me also talk about the discussion that Mr. Clark and I had because he has reached out to me in an effort to get some understanding about these different encryption issues and how Infragard can provide information in the just the way I spoke about in my previous testimony.

In that light, here is the note that Mr. Clark sent to me today. He wants to apologize for not being able to attend the meeting today. He says he feels like he is suffering from a strain of bird flu. I am reading this verbatim from his email. He would like the Advisory Board to know that he will be getting back to you because he is working on some draft language for a bill related to this topic. He expects to get back to you next week. This would be regarding amendments to Nevada Revised Statutes 597.970, the encryption related NRS. This is in the context of the 2009 Legislative session and he wants to make it have some clarification and to make it more clear for businesses so that they know what they need to do to comply with the law.

The current law states, in essence, that when data is transmitted electronically between two parties, the information must be encrypted so that it is difficult for an intercepting party to read the data, except in the case of faxing. If it is an electronic communication, except for faxing, the information is to be encrypted so that it is difficult for an unauthorized third party to intercept and read the information.

SHERIFF HALEY:
Would that exclude government and law enforcement? And, if so, that will be a problem.

MR. VICTOR:
No it does not. It includes law enforcement. There are a lot of issues and that may indeed be one of them.

What it does mean is that it is difficult for a third party to read the encrypted information. For example, there are programs that are available on the Internet for free that can decrypt weak

encryption. There are flaws in the encryption that have been revealed. Somebody writes a program either legitimately as a computer scientist to demonstrate that there is a flaw or illegitimately because they are a bad guy and then that software inevitably ends up posted on the Internet. So is that considered "difficult" or not? If you know where to go to download it and you know how to install that software, you can decrypt the message. Is that "difficult" or not? That is just an example.

There is another one. Faxes are excluded from the encryption requirement of the statute. Well, I happen to have on my laptop right here a competitor to "eFax". If someone were to send me a fax right now, it would come to my laptop via my email program. It would be in a "cleartext" format. If they were to send me credit card or social security numbers, anyone who is getting this electronic traffic along the way on the Internet can open up that file. Is that a fax or is that an email? It is not really clear. What is a fax versus what is a hybrid fax email? There is nothing in the current statutory language to make that distinction.

Today is not the time to get down into some of the weeds of this issue. These are just some of the examples that may mean there is a good reason to clarify the language so that businesses and the appropriate public entities know exactly what to do to stay within the law and more importantly, know what to do to achieve the goal of the law. We do not want someone who is unauthorized able to see confidential information that is transmitted electronically.

I want to thank Mr. Earl for bringing up the gentleman who had his identity stolen while he was in the hospital. His cancer is in remission, by the way, with his cancer. They used some experimental blood treatment. He is a young man. I think he is only 38 or 39 years old and had a rare form of blood cancer.

What we want to do is make sure that someone who is not authorized to see that gentleman's information does not see it. That is the goal of the law. We want to do what we can to make sure that the language of the legislation meets the goal of the law. I will be assisting in any way that I can with Mr. Clark and the Advisory Board as well in getting down in the weeds so that we can have some clarification on that.

AG MASTO:
Thank you, Mr. Victor. Are there any comments or questions from members in the south? Yes, Senator Wiener.

SENATOR WIENER:
Well, I am two for two because that was my bill too. It was part of an omnibus bill that I brought on behalf of this Advisory Board and Ira and I worked on this with them. It was part of a very big package and Bill remembers that we had some snags on this very piece two sessions ago. So I will be very happy to carry this one too in order to take some of the potency out of those weeds. If there is some model legislation or if there is some thing else going on in other states, let me know. Ira and I, we were really in the forefront of trying to address this issue. We need to tweak it and make it more workable so I will volunteer to do that again.

AG MASTO:
Thank you, Senator Wiener.

MR. VICTOR:
If I may, I would like to add a comment, Madame Chair.

Thank you, Senator Wiener, you are absolutely right that we are in unchartered frontiers here in some cases. Fortunately, this legislation does not take effect until October 1, 2008. A lot of organizations are just now getting their heads around it. I know what the reality is going to be. In October, a lot of organizations are going to say "oh, what do we have to do now?"

Unfortunately, based on past experience, a lot of organizations will not do a lot about this. So if we can make this a priority for 2009 then we can get into a good place before we fall too far behind.

AG MASTO:
Thank you, and then just to follow up with Sheriff Haley's concern, Senator, would you be willing to take a look and address the government agencies and our law enforcement and the impact of this to them as well? Yes, Senator Wiener is nodding her head yes to my question. Thank you, Senator Weiner. Mr. Uffelman, do you have a question?

MR. UFFELMAN:
I was just going to add on to what the Senator has said. Back in 2005, during my first session with this bill, that provision initially said that we had about four months to come into compliance. I fought long and hard to get it extended to October 1, 2008.

Then, of course, I went back to the banking industry and talked to their security guys and said "hey, I can see that there is this problem". At that time they said "not to worry, we will have it all fixed by October 1, 2008". Then, roughly three weeks ago, Citigroup contacted me and said "we have a problem." Also, State Farm Insurance I know has a problem.

The problem with encryption as all of you know is that the key has to be at both ends of the electronic correspondence. I encrypt and you decrypt. This can be a problem, especially for the financial service industry where they may not know who the customer is at the other end at the moment that they have encrypted. How do they transmit the key to them to decrypt? Problems like this have come to light. The unfortunate thing is that the law does take effect on October 1, 2008 and the next session does not start until February 2009. So we have almost a year of limbo or six months of limbo that we could find ourselves in some deep trouble.

AG MASTO:
So the grace period was the delay of the effective date? Was that the intent?

MR. UFFELMAN:
Yes, that was the intent. The statute implementation was delayed by October 1, 2008. I suppose we could have gone back to the 2007 Legislative session and said we were not there yet. I do not think that anyone believed us except Senator Wiener and so here we are. This particular section was handled by Assemblyman Bernie Anderson.

AG MASTO:
Thank you very much, Mr. Uffelman. Are there any other comments from members in the south? Are there any comments or questions from members in the north?

MR. VICTOR:
Madame Chair, if I could comment on that? Again, I want to offer the services of Infragard. This is an excellent opportunity for private sector of the banking community and anyone in the public sector to know that Infragard is here to help. We have a meeting session coming up next month. I do not want to speak for the entire Infragard board but I do not think we would get resistance to offering our services or having another special event to help people in the State understand these issues.

There are solutions to these problems. A big part of it is just understanding the intricacies of encryption and then applying the appropriate encryption to the business or public sector problem. So the solutions are out there. It is just getting the help and we are here to help do that.

AG MASTO:
Thank you, Mr. Victor, and thank you for the presentation. I have a request. If the Senator is willing and everyone else who is working on this particular bill, once you come up with the draft

language or amendment would you be willing to bring it back to the Advisory Board and give us an idea? I am hearing yes and Senator Wiener has requested that any suggestions that Advisory Board members have to please let her know as well.

So, thank you again, Mr. Victor. Alright, we are now moving on to Agenda Item 8c.

c. Reimbursement for breach-related costs, explanation and initial consideration.

MR. EARL:
By way of introduction let me first say that Ira brought to my attention initially a particular proposal from Massachusetts that had at least some potential promise to deal with one of the suggestions that Sheriff Gillespie made at the last meeting. That suggestion was to try and think innovatively about how to modify the existing legal or economic regime in order to prevent crimes by putting in place appropriate incentives. These incentives could lead to the prevention of disclosure of information thereby preventing frauds associated with identity theft.

The particular Massachusetts statute which is laid out here in the background working paper in bold print did not pass. In conversation, Bill Uffelman identified for me additional legislative proposals in other states that bear some relationship to the Massachusetts statute.

Very briefly, under certain circumstances the statute would impose liability on a company that was responsible for a data breach. The liability would enable banks to recover the costs associated with having to close accounts or open new accounts and issue new credit cards for people who were possibly affected by the breach. These alleged victims would complain to their banks and credit card companies and say “look, my name is possibly on a list of identities that have been compromised and I want to take these types of actions.”

Now, banks and other financial institutions suffer real costs as a consequence of that. This Massachusetts statute I have provided as a basis of discussion was one of the first in the country to deal with. Now, there are some problems with the Massachusetts statute as it was drafted.

If, for example, a state is willing to impose a regime which raises the cost to a company that has suffered a data breach then that may act as a disincentive to that company to disclose the fact that the data breach has occurred, despite the fact that state and federal law requires it. So one of the questions that Ira and I have discussed is whether it is possible to tweak this statute or develop another statute in such a way so that the particular disincentive to expose the fact that the data had been breached goes away. Let me turn it over to Ira to talk more about it.

MR. VICTOR:
Thank you, Mr. Earl. As an information security consultant out in the field, I have seen countless examples in which organizations have suffered a breach covered by a state or a federal law that would require them to go public. The organization opts to “sweep it under the rug”.

Please understand that my role is like an accountant, I advise and give the information and then our clients decide what they want to do with the information. So I have to sit silently in the room while a discussion can go something like this: “well, we could find ourselves liable but it is going to be difficult for someone who has an identity theft to trace the breach directly back to us.”

Ironically, because of the increase in cyber crime, we have a negative feedback loop. A breaching company could argue that if customer Jane Doe is in our database and her information is breached, Jane Doe could also have been a customer of TJ Maxx where there were 40 million plus records breached. Jane Doe could have been a customer at Citibank, or some other agency, on the list of agencies that have suffered millions and millions of records data breaches in recent years.

The discussions then goes: “well, how would Jane Doe prove that it was us due to the data in our compromised database caused her damage? Therefore, it is not likely that we are going to be sued so we are going to sweep it under the rug.” The conversations go something like that in many cases within many organizations that experience data breaches.

Obviously this does a disservice to the citizens of Nevada. The citizens of Nevada should know if their data has been compromised so that they can take prophylactic efforts to protect their information.

Also, in a perverse way, there are companies that do come forward with breaches and it makes them look worse than other companies. For example, let us take TJ Maxx since that is public. Maybe Jane Doe decides that she is not going to go shop at TJ Maxx today. She is going to shop at “Joe Maxx” today instead and “Joe Maxx” may have had more breaches than TJ Maxx but she does not know that. This creates a moral hazard that acts to preclude “Joe Maxx” from coming forward publicly with their breaches.

So the discussion has been, as Mr. Earl said, how to come up with a potential regime that would incentivize the entity that has a breach to come forward quickly. This is a time issue as much as anything else. When the bad guys get the information, as people in law enforcement know, they will get a fake card or a fake identity out there in some cases on the very same day. They have all the information and all of the machinery in motion to process the identity and create a brand new identity somewhere else in the country, or the world, using that stolen information. So making a fast disclosure is very important.

Maybe there is a way to say to entities in Nevada “if you come forward quickly – 24 to 36 hours fast – then your liability would be capped on the damages that you would have to pay to banks or financial services companies and entities who incur costs for shutting down their accounts.”

We could give them a little carrot and stick. It would be a helpful tool for me to have when organizations are deciding to sweep it under the rug and are saying that maybe it will never get out there. I could say to them that if we announce now, before the clock starts ticking, that they are going to have lower costs than if they keep their fingers crossed and hope that no one is going to sue. Maybe that would raise a few eyebrows in these meetings about whether the organization should just come forward with it and help their customers be protected.

Anecdotally, when I go to businesses on the east coast or in California I notice at every corner that there is a mega bank, Wells Fargo or a Bank of America. When I am here in Nevada there seems to be a lot more smaller community banks here then in those larger east and west coast cities.

It is the small community banks, I believe, that suffer disproportionately from these types of data breaches. They do not have the slack, the staff, and the automated systems in place sometimes to change accounts easily when a breach occurs. They have to go out and hire temporary staff. They have to buy some new software or equipment to respond. They have a disproportionate expense compared to some of the bigger national banks.

I think we would be helping those smaller banks who might not otherwise come forward with a breach issue. Later, when the breach is revealed, the community banks are then scrambling. We are helping those community banks with an expense that is rather large for them. That may be a smart thing for us to do here in Nevada. This would make us a friendly place for those types of entities to do business while protecting the citizen.

AG MASTO:
Thank you, Mr. Victor. Are there any comments or questions for Advisory Board members in the south?

MR. UFFELMAN:
Senator Wiener made mention earlier about the omnibus bill for 2005. It contains provisions that relate to the disclosure of a breach and some aspect of it is built into the Gramm-Leach-Bliley legislation – with the hold harmless provisions – if in fact the entity does disclose the breach.

There is an intertwining of issues here such as the action in Massachusetts that bankers there initially took when they sued TJ Maxx over TJ Maxx's failure to maintain any kind of security system. Nevada law does not deal just with electronic security and not just with credit cards. The Nevada Statute can also relate to health care records that includes personal information.

It was during the discussions of that potential disclosure of personal information, as I recall during the session, that the Department of Motor Vehicles had a related incident in which someone had driven through the wall at one of their locations and stolen a computer with personal information on it. Amazingly, this turned up on the top of a building with a tarp over it like the day after the bill was signed.

The problem that Ira has identified cuts both ways. Your typical community bank is calling the card issuer named in the incident. For example, the Nevada Banker's Association corporate card that I carry is issued by Black Mountain Community Bank, a small community bank over in Henderson, but the reality is that it is a Wells Fargo card. They contract the services through Wells Fargo.

About a year and a half ago, they had to replace it because there was a breach here in Las Vegas. It was never disclosed as to who or what it was but, in fact, the disclosure hit the Wells Fargo system. It may well have actually related back to the TJ Maxx data breach. So Black Mountain had to reissue the card.

The irony at the time was that my present board chairman happened to be the President and Chief Executive Officer of Black Mountain Community Bank and he was in my office lamenting that they had to replace about 3,300 cards that cost about $20. to $25. a card in terms of labor and the like. I told him to sue them because the bank could recover those costs. He said legal action just was not something he would pursue. In effect, such losses are a cost of doing business.

There is a thing called the "interchange fee" that is applied to every transaction that uses the electronic payment system. Whether you use a debit card or a credit card, the rates are different, but on average it is about two percent (2%) of the transaction. As Tray Abney can tell you for on behalf of merchants, the entity or merchant accepting the card also accepts the cost of the interchange fee.

That fee then flows back into the credit card system which flows back to the banks that issued the cards. So in some respects, it was presumed the two percent (2%) fee would cover fraud losses so long as the merchant gets the approval number assigned to that card transaction and absent some fraud on the part of the merchant. So a five dollar ($5.) transaction with a ten cent (.10¢) charge, the merchant gets four dollars and ninety cents ($4.90). That ten cents (.10¢) accrued across the system pays to run the system and pays for the lost card.

The trouble is that when you see the tab for 94 million cards, it looks like a big hit on the system and that is what got people's attention.

Another piece built into this puzzle is related to the payment card industry – VISA, Master Card, AMEX (American Express) and a few smaller ones out there that none of us may know about. They have a set of standards for data retention. Merchants, and anyone who is accepting cards, must follow these Payment Card Industry Data Security Standards (PCI DSS).

These standards establish time limits for how long the merchant can retain that data. There are a whole host of things merchants agree to comply with, once they have signed their card agreements with VISA, Master Card Discover or AMEX.

Two or three years ago, I think, there was a forty-five percent (45%) compliance rate among merchants. The compliance rate now is in the upper mid-ninety percent range (90%), I believe. The industry is quite comfortable with the higher compliance rate. We have achieved implementation of all of this security by nearly everyone.

Just this morning, I got the first message from a grocery chain about an incident. Apparently, the PCI certified security system that this particular grocery store was using was not quite as secure as everybody thought. So now they are trying to figure out if it was an inside job. Did somebody get a key stroke logger to commit a breach, for example? Who knows what happened? Basically, every grocery store in this particular chain transmitting presumed secure encrypted data has been compromised.

It is Friday morning and the industry and the PCI standards are now suspect. So we are back to the drawing board again. This is related to the earlier discussion about encryption. This was an encrypted system and it is now not as encrypted as everybody thought. So it is an ongoing issue.

When a card holder receives a new or replacement credit or debit card in the mail because, to quote "your account has been hit and, by the way, you get a freebie to notify the credit bureaus to put a lock down on your card" – and we have that law here in the State of Nevada – the first person they blame is the bank that sent them that notice with the new card. They do not blame the retailer where the data breach may have occurred. They do not necessarily know that the bank does not necessarily know who was actually responsible for the breach.

Banks have a reputation at risk. Nevada law does provide for a civil action to recover costs, to the best of my knowledge. However no one has pursued this in Nevada. The reason would evolve into one of these egregious situations. Banks may have said, "yeah, you know, they stamped it certified but they have done nothing and, by the way, they have retained every record for the last ten years for every credit card that they swiped, they ought to have to pay. However, a lawsuit is not something that we want to fund ourselves every other week."

I hate to say it but there are breaches all the time in lots of places as small or large as you want to go out and find. I do not know whether Nevada needs new legislation or not. I think it is one of those cases where this is international in scope. We need to figure out how to do it because the bad guys are everywhere.

AG MASTO:
Thank you, Mr. Uffelman. Are there any further comments from the Advisory Board members in the south? Hearing none, are there any comments from the Advisory Board members in the north? Yes, Mr. Victor, please continue.

MR. VICTOR:
In concludion, the thinking is that we want to incentivize entities that have a breach to come forward quickly. We know there are a lot of breaches. As the saying goes in security, nothing is 100% secure. I tell my clients to give me all their data and I will put it in one of those big shipping containers that go across the ocean. Then I will fill it up with concrete and I will drop it off a bridge. Then I will guarantee that no one will get into it for 30 feet or 30 days, whichever comes first. Short of that, we can not keep something 100% secure.

What we can do, though, is incentivize entities to come forward so that people who face potential harm from a breach can take action to protect themselves quickly to minimize any damage that may occur.

I think that Senator Wiener was excellent a few years ago in her efforts. She and I talked about this bill a few years ago to require the notification of breaches. I am thinking that we may still need a bit more of a "carrot and stick" approach to get that notification really out there and get it out there quickly.

AG MASTO:
Thank you, Mr. Victor, and thank you for the presentation. Moving on to Agenda Item 9, it is time for general comments from Advisory Board members.

Agenda Item 9 – Board Comments

SHERIFF HALEY:
Thank you, Attorney General Masto. I have questions relative to NRS 179.1211 concerning forfeiture as it relates to this particular Advisory Board. Does anyone know how robust the courts have been in this particular area about ordering forfeitures? Is any criminal case of a technological nature submitted by any agency automatically a tech crimes forfeiture case? How does that occur?

AG MASTO:
Thank you, Sheriff Haley. Mr. Earl, would you like to try to address those questions?

MR. EARL:
I will try. To my knowledge, despite some educational efforts that we have put in place since the passage of the new forfeiture bill (Assembly Bill 306) in the last Legislative session, there has not been a prosecution that involves tech crime forfeitures. I see this as a result of the very large challenge that is posed to law enforcement in the first instance to recognize the importance of electronic related events. The cop on the street must recognize evidence, safeguard it appropriately, and get it to a criminal computer forensics lab to be able to be analyzed.

The second tier of education is one that has to take place with prosecutors all over the State. This involves understanding that electronic evidence is, or can be, vitally important in proving a case. Also, if a prosecutor is working hand and glove with a law enforcement agency, whose cases that prosecutor handles, and that prosecutor recognizes a potential case as involving technological crime, then charging under the forfeiture statute in addition to the overriding criminal offense is at least a possibility. If appropriate charging occurs then other consequences follow.

Despite some of the information and some of the news that surrounded the passage of AB 306, to my knowledge, there has not been a case that has been prosecuted at all either successfully or unsuccessfully. So in terms of how this actually works, we do not have much in the way of history. Quite frankly this is a significant educational challenge for the Advisory Board, for law enforcement and for prosecuting attorneys across the State.

SHERIFF HALEY:
Thank you. That answers my question.

AG MASTO:
Are there any other questions or comments from the Advisory Board members? Hearing none, we will move on to Agenda Item 10.

Agenda Item 10 – Public Comments

AG MASTO:
Are there any members of the public in the south? Please come forward at this time to address the Advisory Board. Seeing none in the south, are there any members of the public in the north who would like to address the Advisory Board? Seeing no one in the north, we will move on to Agenda Item 11 and turn this over to Mr. Earl.

Agenda Item 11. Issues for next meeting, scheduled June 13, 2008 at 10:00 am.

a. Board Elections for Chair and Vice Chair

MR. EARL:
Thank you, Madame Chairwoman. I just want to highlight for the Advisory Board's attention some of the issues that we need to face and be thinking about in the interim before the next meeting. The Advisory Board statute requires an annual election for Chair and Vice Chair. Historically, the Chair has been the Attorney General but those elections do need to be held at the next meeting.

b. Program funding.

I am always open for suggestions to issues or items to be placed on the Advisory Board's agenda. There is a standing invitation to Advisory Board members and others as well to let me know what might need to be addressed. I am interested to find out what programs the Advisory Board might be interested in supporting in one way or another. This is particularly relevant to new members.

At this time two years ago in the Legislative session, the Advisory Board instituted a mission review that led to a questionnaire that was sent out to law enforcement all across the State. One of the ultimate results of that was the Advisory Board's recommendation that additional personnel be added to the Attorney General's Office which was successful in the Legislative session.

There may be some additional programs, not necessarily that the Advisory Board would need to fund, but that it might facilitate in some way. This might e legislation or simply a discussion among Advisory Board members about areas for cooperation.

c. Budget

Also at this time two years ago, it was the first time that any Executive Director had addressed an Advisory Board budget with this board. I want to do so with this Advisory Board in this Legislative session as well.

You need to be aware that the Advisory Board's budget is put forward to the Legislature through the Attorney General's Office itself. Advisory Board members who have been here for awhile will recall that way back in August I distributed a working paper that talked about Advisory Board finances. It had been cleared by the Attorney General's Chief Financial Officer and Chief of Staff at the time before it went out to any of you. I just wanted to raise that. You can expect to see from us some issues dealing with the Advisory Board and how it functions and whether there is money that will need to be requested from the Legislature.

d. Other

In terms of other items again, I am open for suggestions. We did try and plan, at the suggestion of the Advisory Board, meetings scheduled throughout the year. We have not scheduled a date yet for December 2008. We have a date to which most members have agreed but it falls within the time period that the Legislative facilities are normally closed in preparation for the Legislative session. So, looking forward, I may call on the assistance of our Legislative members to provide some assistance so that we can have a December meeting in these facilities.

We also need to think about where and how the Advisory Board will meet during the first quarter of next year which is when the Legislature is in session. An earlier meeting might be necessary if the Board wants to consider legislation introduced by the commencement of the session.

That is all I have with regards to the heads up for the next meeting.

AG CORTEZ MASTO:
Thank you, Mr. Earl. Are there any questions from the Advisory Board members?

SHERIFF HALEY:
Just one more question, Madame Chair. Back to my earlier comment, I had talked to Jim about approaching and getting on the agenda of the Sheriffs and Chiefs meeting where the prosecutors and the sheriffs and chiefs meet in the summer to talk about this forfeiture issue and how we can all educate ourselves about that. I would like to approach them and see if we can get on their agenda. If you or Mr. Earl would let me know the appropriate way to do that for the Advisory Board I would appreciate it.

AG CORTEZ MASTO:
Thank you, Sheriff Haley. Actually, I can make a recommendation since the Executive Director for the Prosecutors works in my office, Brent Kandt. We can definitely reach out to him through that avenue. Obviously with Frank Adams of the Sheriffs and Chiefs Association and through Mr. Earl, maybe we can set up a meeting with both of them to request that this item be put on their agenda for their combined meeting this summer.

SHERIFF HALEY:
Thank you, I think that is a good venue for us to do that.

AG CORTEZ MASTO:
Thank you, I agree. Are there any further comments or questions from the Advisory Board members? Hearing none, we move on to Agenda Item 12.

Agenda 12 – Adjournment.

AG CORTEZ MASTO:
I pronounce this meeting adjourned. Thank you.

Meeting adjourned at 11:50:00 AM.

Respectfully submitted,

_Ursula K. Sindlinger____
Board Secretary

Approved by the Board at its subsequent meeting on June 13, 2008.

Minutes of the
Nevada Technological Crime Advisory Board

June 13, 2008

The Nevada Technological Crime Advisory Board was called to order at 10:00 a.m. on Friday, June 13, 2008. Attorney General Catherine Cortez Masto, Chair, presided in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in Room 3138 of the Legislative Building, Carson City, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Chris Ipsen *(Rep. for Dan Stockwell, Director, NV Dept. of Information Technology)*
Lt. Tim Kuzanek *(Rep. for Sheriff Mike Haley, Washoe County Sheriff's Office)*
Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)
Dale Norton, Nye County School District Assistant Superintendent
Nevada State Assemblywoman Peggy Pierce
Special Agent Rob Savage *(Designated representative for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS))*
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)
Nevada State Senator Valerie Wiener

ADVISORY BOARD MEMBERS ABSENT:

Gregory Brower, U.S. Attorney, Department of Justice (DOJ)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)

TASK FORCE MEMBERS PRESENT:

Detective Dennis Carry, Washoe County Sheriff's Office

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director
Conrad Hafen, Nevada Chief Deputy Attorney General, Advisory Board Counsel
Ursula Sindlinger, Board Secretary

OTHERS PRESENT:

Mohamed Humaid Al Mualla, Forensic Security Manager, United Arab Emirates
Nawaf Mohamed Almouada, Chief Public Prosecutor, Bahrain
Petra Apsner, Assistant State Prosecutor, Slovenia
Joe Majka, Senior Business Leader of VISA Cyber-Security Investigations
Markas Marcinkevicius, Head of Second Division, Lithuania Criminal Police Bureau
Antonio Nascimento, Diplomatic Advisor to the Prime Minister, Cape Verde
Herinavalona Thierry Ravalomanda, Magistrate, Madagascar
Norma Reyes, United States Department of State, International Visitor Leadership Program, English Language Officer
Iipumbu Wendelinus Shiimi, Assistant Governor, Bank of Namibia, Namibia
Jack Williams, President of eCommLink

Agenda Item 1 – Call to Order - Verification of quorum

AG CORTEZ MASTO:
This meeting is called to order on June 13 at 10:00 AM.

A roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Discussion and approval of minutes from March 28, 2008 Advisory Board Meeting.

Motion to approve the minutes was made by Senator Wiener and seconded by Assemblywoman Pierce.

Motion to approve minutes passed unanimously.

Agenda Item 3 – Annual election of Chair and Vice Chair.

MR. EARL:
The advisory board statute requires an annual election of both the positions of Chair and Vice Chair. It is open to you, Madame Chair, to ask for nominees for the position of chair.

AG CORTEZ MASTO:
Thank you, Mr. Earl. Are there nominations for the position of Chair?

Motion to approve nomination of Attorney General Catherine Cortez Masto as Chair was made by Senator Wiener and seconded by Mr. Uffelman.

Motion to approve the nomination passed unanimously.

AG CORTEZ MASTO:
Thank you, we have a Chair. Now, I will entertain nomination for the position of Vice Chair.

Motion to approve nomination of Senator Valerie Wiener as Vice Chair was made by Mr. Uffelman and seconded by Assemblywoman Pierce.

Motion to approve the nomination passed unanimously.

Agenda Item 4 – Report regarding Northern Task Force Activities.

AG CORTEZ MASTO:
Do we have a report with respect to the Northern Task Force activities?

RAC WHITE:
We recently conducted a mid-year evaluation of the digital forensic positions. We have one full time position in Reno, Special Agent Melissa McDonald. We also have with us a state-funded computer forensic analyst, Talova Davis from the Attorney General's Office (AGO). Ryan McDonald, a computer forensic investigator from the AGO and one part-time Federal Bureau of Investigations (FBI) agent, Anna Brewer, also work on the Task Force at our facility at Immigrations and Customs Enforcement (ICE) office in Reno.

The Northern Task Force has handled 32 cases most of which involve child pornography investigations conducted at both the federal and state level. During March they assisted with ten search warrants that the County and the FBI led.

Most recently, we had two investigations involving child pornography where all entities assisted in the forensic evaluation of computers. One case involved over 20,000 images and numerous

video clips of child pornography. Another case involved over 5,000 images. Both are proceeding to indictment on the federal level.

At this point, we have a very good working relationship established. The addition of the State computer forensic officers to the Task Force has allowed our federal officer, SA McDonald, to actually focus a little bit more on ICE cases and to compartmentalize the State and local cases. It has become a more cohesive unit with the addition of Ms. Davis and Mr. McDonald.

MR. EARL:
Madame Chair, I think that Lieutenant Kuzanek who is substituting for Sheriff Haley also has some information regarding the functioning of his unit. He heads the northern fusion center.

Lt. Kuzanek:
Madame Chair, I am glad to be here today representing Sheriff Haley. In my capacity as a Lieutenant with the Washoe County Sheriff's Office, I am also assigned as the Director of the Northern Nevada Counterterrorism Center.

To provide you with an update of where we stand, operations from construction through product development have come a long way since February. We initiated operations that are identifiable. We began in early February and we continued to pick up speed and we have begun to deliver advisory bulletins and other products on a weekly basis now.

The Fusion Center in the north continues to develop and take advantage of the numerous relationships between the different agencies including those in the government realm. Those agencies include the Southern Nevada Counterterrorism Center through Las Vegas Metropolitan Police Department, and the State Fusion Center as it begins to stand itself up.

We are working with a number of other agencies in the private sector as well. We communicate daily with representatives from the casino and hotel industries and many others.

In many ways, what we anticipated I reported earlier in the year to numerous committees is actually starting to occur now. We are very encouraged that the cooperative relationships that are being built just continue to expand and it has really gone well. Thank you.

AG CORTEZ MASTO:
Thank you, Lieutenant. Are there any other comments from the Northern Task Force members? Hearing no further comments, we move on to the next agenda item.

Agenda Item 5 – Report regarding Southern Task Force Activities.

SAC MARTINEZ:
I am here to report on some of the investigative activities of the Southern Task Force.

First and foremost, I want to mention that on May 22, a Henderson man was indicted by a federal grand jury in Roanoke, Virginia for sending email threats to two Virginia Tech alumni on the eve of the one year anniversary of the University's mass shootings. The investigation was primarily conducted in Nevada jointly with FBI, the College of Southern Nevada, and the Henderson Police Department. This was something that ran substantially under the radar mainly because we were very concerned about keeping this person incarcerated.

Henderson Police Department was very instrumental in finding the means by which to have a psychological evaluation ordered. In the meantime the U.S. Attorney's Office in Roanoke, Virginia was able to get a true bill indictment and that individual either has or will be remanded to authorities in Virginia.

Backing up a little bit to early April, I have a case I want to highlight that will give you an idea of the level of technology sophistication that even child pornographers have.

A man was indicted in federal court on one count each of transportation, receipt and possession of child pornography. He created a password-protected folder on a Russian website and used it to store child pornography he possessed. He then obtained and distributed additional child porn by exchanging his folder name and his password for those of other individuals on the site to access.

This individual used publicly accessible College of Southern Nevada (CSN) computers to access the site. We had full cooperation and extensive assistance from the CSN Police Department in this case. A dozen Apple Mac computers were obtained for forensic analysis. You have heard briefings in the past about the level of difficulty that exists when that much media is being examined. That forensic analysis was successfully completed by the Southern Task Force.

This individual was arrested while using a CSN computer to access child pornography. He had several USB (Universal Serial Bus) thumb drives in various sizes up to one gigabyte in his possession at the time of his arrest. The level of sophistication of computer forensics involved in this case is high, especially where a child pornography distributor here is using a Russian website to maintain his portfolio of child pornography.

In a separate case on May 28, a woman was indicted on one count each of receipt and possession of child pornography. She had obtained the child pornography through various online news groups. It is rare to have a woman involved in this type of activity. That is not to say it does not happen.

In this case, the information came from the woman's sister who was very concerned for the welfare of children in the home. This was a successful case but very unusual because of the individual in possession of the child pornography was a woman.

On June 3, a man entered a guilty plea on one count of receipt of child pornography. The investigation was initiated into this individual's activities on an online message board that is advertised as a place for "kiddie-lovers around the world."

The message board was infiltrated and monitored by the FBI and its participant users were identified. When the search warrant was executed, the subject's residence was actively accessing child porn at the time. The child porn was displayed on his computer monitor.

The last case I wanted to mention involved a man who was found guilty on one count each of coercion and enticement of a minor and interstate travel with intent to engage in illegal sex acts with a minor. Of note in this case is the man had hundreds of stories regarding having sex with minors and incest stored on his PDA (Personal Data Assistant) when he was arrested and the PDA was seized.

On May 13, FBI Supervisor Special Agent Eric Vandersteldt, the supervisor managing the Southern Task Force, and Lieutenant Bob Sebby from Las Vegas Metro Police Department made presentations regarding cyber threats at the Technology Summit in Las Vegas sponsored by the Institute of Electronics and Electrical Engineers Computer Society.

This is a highlight of the recent work that has gone on with the Southern Task Force since our last meeting.

AG CORTEZ MASTO:
Thank you, SAC Martinez. Are there any other comments from any other members of the Southern Nevada Task Force? Hearing no additional comments, let us move on to the next item.

Agenda Item 6 – Overview and update of InfraGard activities.

SAC MARTINEZ:
Madame Chair, Special Agent David Schrom was scheduled to give this presentation. Unfortunately, he is not able to be here with us today due to a personal emergency which requires his attention. Those of you who know Dave know that he has been an absolute ball of fire in keeping our InfraGard program going. Dave will be very disappointed that he was not here to make this presentation. I will see about getting you a report at the next meeting.

AG CORTEZ MASTO:
Thank you, SAC Martinez. Obviously we are very sorry to hear this news. Please give SA Schrom our best. We wish him a speedy recovery.

MR. EARL:
Madame Chair, before we move on I would like to add something which I think David would have brought to light. Board members will recall that the presentation he was planning on giving was essentially the second half of our look at Infragard. The board heard a report from Ira Victor, head of the northern section of Infragard, at the last meeting.

The significant update that occurred after the last board meeting was an Infragard meeting in which the attendance had tripled. The participation by public and private sector at the Infragard meetings in the north has normally run about 30 to 40 people in attendance per meeting. After the discussion before the board, attendance jumped to over 100 at the following Infragard meeting.

Ira attributes this largely to the efforts of board member Trey Abney in terms of putting out the word through the Reno-Sparks Chamber of Commerce sources. I just wanted to draw the board's attention to this fact that the last meeting had its desired effect here in the north in terms of greatly increasing the private sector participation.

MR. ABNEY:
I would like to add that the last meeting was the first time I met Ira Victor and right after the meeting we started discussing hosting a joint Chamber member and Infragard member meeting on protecting data from fires and earthquakes. That presentation was very poignant and timely.

The idea was to expose the Chamber members to Infragard and get them up to speed on what was going on and to encourage them to join the effort. This also provided an opportunity for Infragard members to learn a little bit about the Chamber. It was a successful event and we hope to do more things like this in the future. Thank you.

AG CORTEZ MASTO:
Thank you. That is great news and I appreciate all of your effort and work you put in to that, Trey.

Now we move on to Agenda Item 7.

Agenda Item 7 – Pre-paid debit cards and the challenges they present to law enforcement.

AG CORTEZ MASTO:
First I would like to introduce the following presenters under this agenda item, Jack Williams, President of eCommLink, and Joseph Majka, Senior Business Leader of Cyber-Security and Investigations with VISA.

MR. MAJKA:
Madame Chair, my name is Joe Majka and I am a Senior Business Leader at VISA Inc. I have global responsibility for fraud investigations and cyber security for VISA throughout the world. My team primarily responds to computer intrusions where merchants, processors, financial institutions and any entity that is storing or processing VISA transaction data that has been

breached and data is stolen. I also deal with any type of fraud situation involving VISA products and VISA cards throughout the world.

I will let Jack Williams go first with an update on “pre-paid” issues. I will answer any questions you may have at that time regarding VISA activity and pre-paid cards.

MR. WILLIAMS:
Good morning, Madame Chair. I appreciate the opportunity to present about pre-paid debit cards. Let me first start with a little bit of background about myself.

I am the one who invented the very first gift card in the world in 1993. I invented the first electronic gift card while at Blockbuster Entertainment. I can not tell you how many guys came to me and said, “you saved my marriage because now I can buy an easy gift for our anniversary”.

In those days, when gift cards were first beginning, it was a very difficult process because people did not care for gift cards. Today over $250 billion dollars is transacted on gift cards in the United States on both the “closed loop” or merchant specific gift cards and what we call the “open loop” or branded cards with MasterCard, VISA or Discover logos on them.

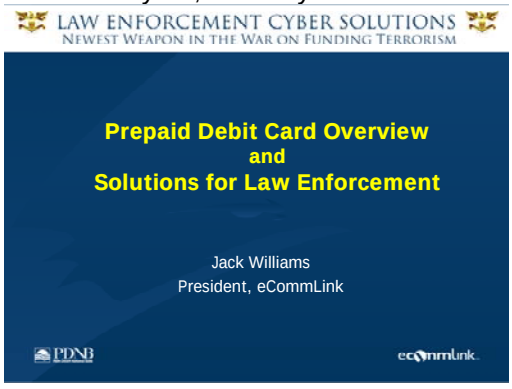
I am on the Federal Reserve Board payment card committee. I am the subject matter expert for “pre-paid” cards. Also I work on the federal level with the United States Department of Drug Enforcement Administration (DEA) and I am starting to work with the United States Treasury.

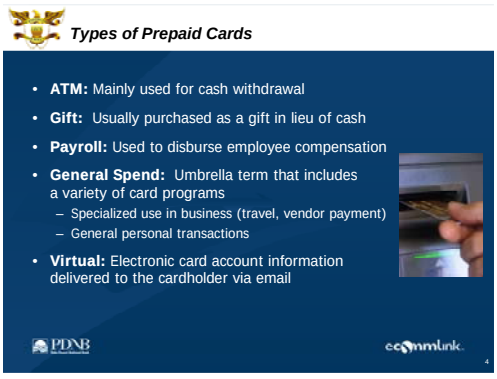
The Financial Management Service Bureau of the U.S. Treasury (http://www.fms.treas.gov/) was involved in the design of the Social Security pre-paid debit card that is being launched by Coamerica (http://www.coamerica.com/), a MasterCard product.

I do not have the VISA slant but I am very much involved in many different areas of law enforcement. I work with Lieutenant Bob Sebby here at Las Vegas Metro in trying to unravel some of the interesting nuances because pre-paid cards have changed.

If you remember back in the late 1990s, pre-paid cards were used as an instrument for gift cards. It was something that you had to ask for when you walked into a store, even those that had them. Certainly, gift certificates were even less used before that.

Today, when you walk into a store, for example, Safeway or Kroger, you can buy pre-paid gift cards. Last year, Safeway alone sold a billion dollars worth of other merchants’ gift cards.





What is changing in the world today is the migration from a gift card to conducting financial services on a pre-paid card. For example, I can tell you that on this cell phone card today, I can move money from anywhere in the world to any else in the world in five seconds. I can move unlimited amounts of money all because eCommLink is a prime core processor for pre-paid debit cards.

I bring before you an extensive knowledge base on the subject of pre-paid cards including what they can do and how they work. I would also like to show you a dilemma that law enforcement faces today and a proposed solution that we have talked about. Lieutenant Sebby and Las Vegas Metro has been very much involved in helping us with this.

We host a law enforcement “pre-paid card 101” course on almost a weekly basis. Our offices are here in Las Vegas, located very close to the car rental center, to give you a physical point of reference. We work closely with law enforcement and not just with the fraudulent use aspect that VISA will speak to.

I am also involved with what we will call the “money-laundering” side of pre-paid cards. In addition, I work with Special Operations Command out of McDill Air Force Base, which is involved with investigating the terrorist funding use of these pre-paid cards.

There are three different genres of pre-paid card applications used by the “bad guys”. For the next ten to fifteen minutes, I will give you a quick overview.

We have talked about eCommLink a little bit. We are going to talk about the overview of the cards and then we will talk about a platform that might be of interest to you.

Briefly, as eCommLink, we are considered to be the experts in the pre-paid card field. It is nice to be here in Las Vegas. I moved here last year from Washington D.C. This has been a delightful change.

At eCommLink, we process millions upon millions of transactions every year from all over the world. We process MasterCard, VISA and Discover transactions that can originate literally anywhere that these credit cards are accepted. We are very much involved in the mobile transaction, which is a new category and new threat on the horizon.

Last week I was a speaker at the National Anti-Money Laundering Conference in Washington D.C. and there were maybe about 1,000 law enforcement professionals from every organization in attendance.

The mobile transaction issue involves moving money by cell phones from one place to any other place in the world. This has caused consternation at the very lowest level and, at least, a lot of interest in how the “bad guys” can use this. The good news is there is a countermeasure and we will talk about that today.

We are a Microsoft processor. We have all the certifications that are required. We are actually one of the few companies that has all the certifications. We are also audited by the Federal Deposit Insurance Corporation (FDIC) and by the Federal Reserve Board. We would like to think we are bringing knowledge to you that represents many years of understanding in this field. We are one of the cutting edge processors and providers.

Briefly, these cards represent a certain threat threshold that we are going to begin to see more of and not less and less of. We talked about child pornography earlier. Money, as Joel Grey sang, makes the world go ‘round. Money is certainly the nucleus of bad intentions.

With World Bank, we were able to break up a child pornography funding ring. They had used pre-paid cards to create a private network for moving significant amounts of money anonymously. It ties in to this cutting edge of Russian websites mentioned by the FBI today and “smurfing” all of the sites so that you would go halfway around the world before you end up in Russia.

The kinds of cards that exist today include ATM (Automated Teller Machine) cards. These are cards that have a PIN (Payment Information Number). Gift cards are non-reloadable, the kind you would give to somebody as a gift.

The hottest and fastest growing cards are payroll cards. Numerous employers around the United States are migrating from paper checks to payroll cards to pay their employees. I would say that even the State of Nevada has moved to using these cards for disbursement of funds to the unemployed.

I am a commissioner on the Electronic Benefits Transfer (EBT) Commission for the State of Texas, I am a sixth generation Texan so we cannot lose all of our roots. Texas is moving aggressively to migrate all payments to pre-paid debit cards.

The cost model for that example is that it is free to the State. Who pays those costs? Nothing is free. The merchants who accept the cards pay for it and it is called “interchange”. You may see different merchants involved in various lawsuits because their perception is that they are over-paying for the cost of the services that VISA, MasterCard and Discover provide. This payment can also be used to offset the cost of funds disbursement.

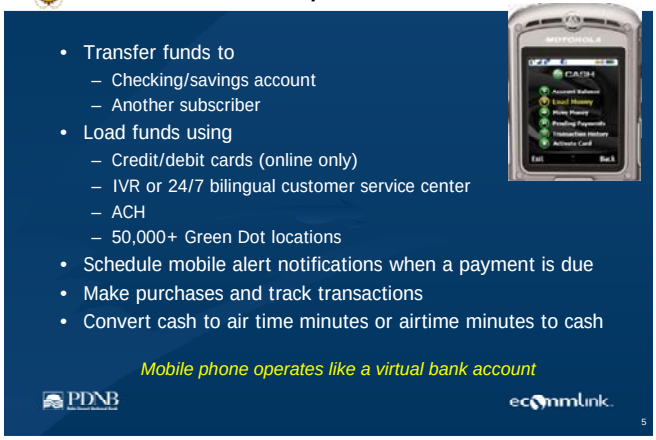
You will see many states moving to pre-paid cards rather than paper checks and as are other employers. Basically, the model is that it is free to the employer and the merchant pays the processing costs. General spend cards are the most common. This is a card that is not endorsed by an employer but it is a card that has the full functionality of a credit card.

I can do everything using an eCommLink pre-paid debit card that I can do at financial institutions. That is the dynamic that is changing. Usage includes not only debit card point of sale (POS) purchases but bill payment, savings accounts, and international funds movements. The functionality normally reserved for traditional banking services is now migrating to these cards.

Not only do we operate in the physical space with a piece of plastic but also in the virtual space. If you go to www.discover.com today, we process here in Las Vegas all of the virtual Discover gift cards. You can go online and buy a card for somebody for up to the $500. and literally, in 5 seconds, they will have the card and they can be online using that card for whatever acquisition they want to make.

Mobile commerce is the hot thing. It is something that we are considered to be on the cutting edge of. We believe very strongly that we need to be aware of it.

Mobile Commerce Capabilities



Today, using a cell phone that is tied to a pre-paid card, I am able to transfer funds from anywhere in the world to a checking account, to a savings account or to another subscriber. For example Madam Chair, if you had an m-cash card, which is what we call this, you could easily use your cell phone number to move money. It can also be done very quickly in the merchant community. Any account can be used for this.

For example, today if you have a child in college and need to get money to him or her quickly, this method gives you the convenience of doing this easily. I have daughter who spends my money all the time. I used to be able to say “I cannot get to a computer so I cannot send you any money”. However, today she knows I have account access through my cell phone so I can do it in seconds. I am not really sure I should have invented this, the idea of being able to load funds and move funds. Moving cash through networks has proliferated.

In today’s environment, Wal-Mart, Safeway, Walgreen’s, Radio Shack and numerous other merchants allow for the loading of cash that can be credited to a pre-paid card and accessible through a mobile cell phone.

Bad guys can use SMS (short message service) text messaging to convert air time into dollars and dollars into air time. This is not only a domestic phenomenon but this is becoming a worldwide phenomenon.

We have customers all over the world who use SMS for money remittance and money transfers. Philippine employees in this country may need to move money because they are supported by the Philippine government. Twenty percent of their “take-home” has to be sent back to the Philippines. They use cell phones in order to accomplish that transfer quickly and conveniently. In seconds someone in the Philippines can access the money sent from the U.S.

Let us talk about the bad guys for a second. These cards and the m-cash methods of transfer are becoming their profit method of choice. It is certainly a lot easier than moving bulk cash. To give you an idea, a million dollars of hundred dollar bills weighs 30-pounds. Not that I go around weighing million dollar chunks of hundred dollar bills, but I do know that bulk cash smuggling has its limitations. Cash is difficult to conceal.

Quite frankly, we could move millions of dollars on a small card very quickly and very easily. Soon, we will be able to download the data now on a card’s magnetic stripe to a PDA or a cell phone using the MP3 music environment.

Federal and state law enforcement agencies are finding more and more of these cards. They face a dilemma because these cards are now preferred by criminals, but law enforcement does not have the tools or knowledge to deal with the cards effectively.

Many times the response from some in the issuing community is “just call the number on the back of the cards.” Unfortunately, the way things are moving, not only do we have the ability to put money on to a card that looks like a VISA card or a MasterCard, but we can also put money on hotel room keys. Any magnetic data, any magnetic stripe that is on the back of a plastic card can be re-encoded with the data and the information needed to perpetuate these crimes.

I can go on eBay and actually buy a card re-encoder, I can take a fairly powerful magnet to the back of a legitimate card and demagnetize the magnetic data. I can re-encode it using a device that sells for about $243. Because card re-encoders are so inexpensive, any magnetic stripe on a piece of plastic represents a threat opportunity.

In talking with Lieutenant Sebby, I found out that here in Las Vegas approximately 14,000 cards were confiscated in various criminal investigations. Unfortunately those cards were destroyed but the cards may have had value on them. Without the piece of plastic and the numbers on them, the money was either taken out of the account by the bad guys or was kept by the financial institution.

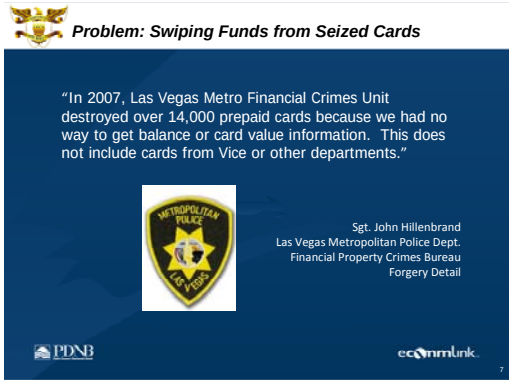
Las Vegas Metro, DEA and ICE face the problem of what to do with all of these cards. I have received calls where an arrest was made and the bad guy had a suitcase full of pre-paid cards. I was asked, “Now what to we do with them? How do we confiscate them?”

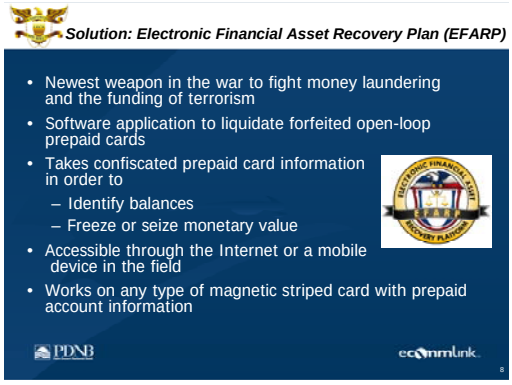
There is another dilemma that is faced at a federal level. When I cross the borders of this country, a law says I can carry no more than $10,000. in cash. However, I can tell the ICE agents at the border that I have a million dollars on my card and there is nothing that they can do about that.

The Financial Crimes Act of 2007 was introduced to deal with this problem. It has been delayed by various agendas. The Act would identify pre-paid cards as monetary instruments. This is an issue that I understand Mr. Earl wants to address.

We at eCommLink asked “What can we do for law enforcement that would empower law them to be able to take this money and confiscate it in an easy and efficient manner?”

As we looked into the solution, we realized the process would have to be readily available because of a federal agenda that I also serve. It would need to be a process that could be done anywhere in the world.



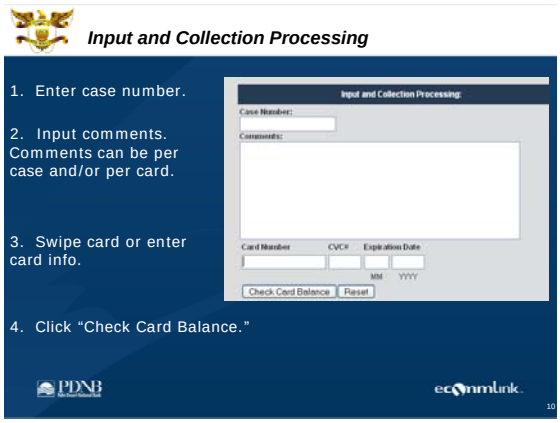


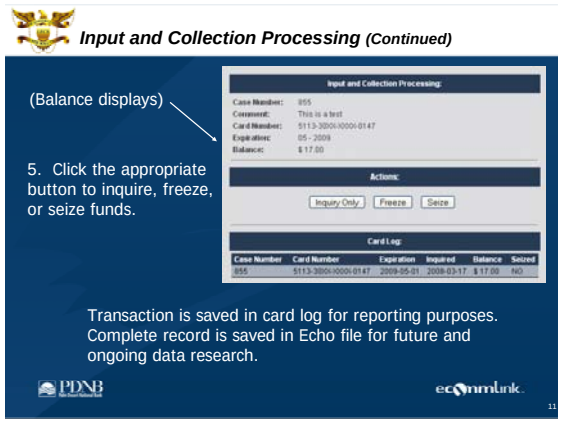
As a result, we sat down and created a program that we call an Electronic Financial Asset Recovery Plan (EFARP) in partnership with Palm Desert National Bank (https://www.pdnb.com/) located in Palm Desert, California. Palm Desert Bank is authorized to do business at the federal level. Working with them, or another national bank, makes compliance with U.S. Treasury regulations less of a problem.

This program would allow a law enforcement officer from anywhere in the world to log in using a password and use another layer of validation. As you can see on the slide, there is a security code that would have to be read and re-entered. This dual source authentication would prevent intrusions and hacking.

The agent would enter a security code, login and password. Once logged into the system, the agent would be able to reference a case number and add relevant comments. The officer would type in the card account number and the Card Security Code (CSC), sometimes called Card Verification Value or Code (CVV or CVC), which is a three-digit number that is usually in the area of the magnetic stripe on the card. (http://en.wikipedia.org/wiki/Card_Security_Code)

After entering the necessary information, the officer would click the "check card balance" button to obtain the amount of money associated with the card. This system would enable the law enforcement officer real time account balance information from the account regardless of wherever in the world the account is maintained.





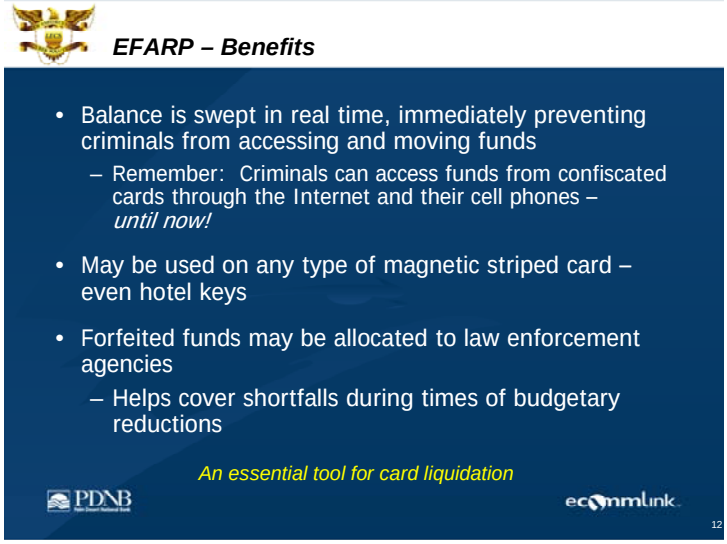
I can access this functionality on a cell phone, a PDA, a laptop, or on a fixed Internet connection. The plan requires nothing to be purchased by any law enforcement because it is Internet accessed at the officer level. eCommLink secures the data that you see on the slides. We can recall the case number that the officer entered. We can recall any comments the officer entered on the case. We can give provide the card number, the expiration date and the balance in real time within 5 seconds so the bad guys don't have the opportunity to move any funds.

We can also freeze and seize the funds shown on the account balance. "Freeze" means that we would put a hold on the funds using a special kind of transaction that looks like a "pay at the pump" or a hotel transaction. The money becomes inaccessible to anyone else. Once the funds have been frozen, eCommLink waits for instructions from law enforcement, pursuant to a court order, before moving the funds. After the freeze, the money is just sitting in an electronic state at the financial institution that is holding it.

The program also has the opportunity to seize the funds. eCommLink would then take the money and put it into Palm Desert National Bank, for example. The money would be held by a national bank awaiting instructions.

We also have the ability to move the funds into an institutional account pursuant to a process that ties the individual's password and login to the institutional account. For example, I can tie Lt. Sebby's login to the Metro Financial Crimes Unit and to a bank account that the unit controls. We move money, billions of dollars, into tens of millions of accounts. eCommLink just needs to know what to do with the funds and when to do it.

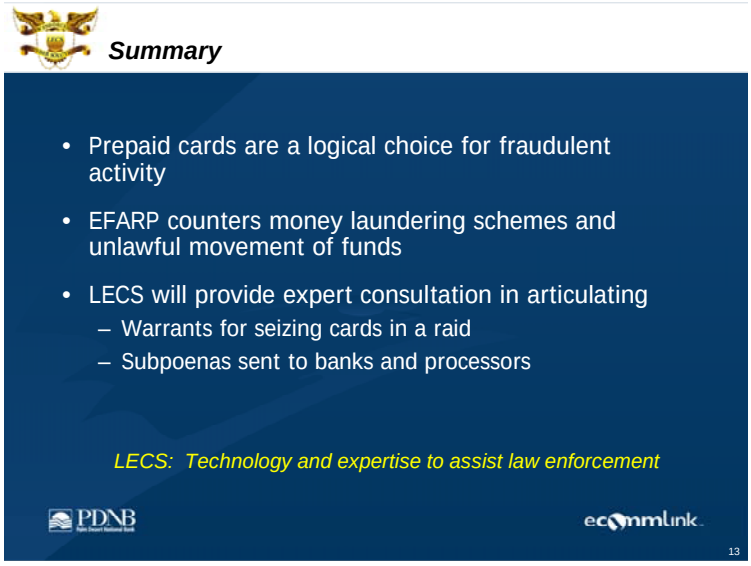
Technologically, eCommLink can seize funds or freeze funds. We do not make that decision. The law enforcement officer makes that call.



When the balances are swept, it makes no difference what the piece of plastic appears to be. What I care about is, whether it is a card with a VISA logo on it or a store pre-paid card. What is important is what they have encoded on the magnetic stripe. You may have been in a Home Depot and they have asked to see your credit card before you swipe it. This is because it is very easy to re-encode the magnetic stripe with different information then what you see is embossed on the face of the card. This is a very popular technique of the bad guys. Home Depot is looking to ensure the encoded information is the same as the embossed information on the card.

All law enforcement needs to be able to do is the swipe cards. If eCommLink can read the magnetic data then we can extract and use the data contained in the magnetic stripe regardless of who placed it there.

In summary, eCommLink has not only the ability to extract the funds that are on these cards but also to start build a database of cards that have been involved in fraudulent transactions, both domestically and internationally. That database is called a shadow file or an echo file. This is important to federal law enforcement because the database could be used to discern patterns of usage. The first six digits of a card number contain significant amounts of information about that card. It tells me which bank is involved. That is called a BIN, Bank Identification Number, or sometimes the Issuer Identification.



If you give me the first six digits of a card number, I have a lot of information, but it is all non-personally identifiable data. None of the information that I can extract from the BIN can be used to identify a person.

It is a card number. It relates to an amount of money. I have no way at all of obtaining the individual information, but I can tell you who the bank is by looking at digit places of seven, eight and nine of the 16 digits. Those are called BIN extensions in our vocabulary. That tells me who the processor is or it tells me who the independent sales organization or other organization is that is using that card.

I have been involved in the writing of numerous federal subpoenas to make sure that the right information is requested. Law enforcement needs the name and address of the financial institution technically owns this data. All subpoenas need to be addressed to the financial institution involved in order for the legal process to run its course.

At eCommLink, we believe that we are able to help law enforcement because we are ahead of the game so far. The bad guys are pretty smart in this area. We are talking about dollars that move and have three commas. It should be understood that are dealing with significant money. This is not small numbers.

We are seeing more bad cards from certain financial institutions then from others. It is my opinion that the threat is not from the major core processors, such as my company, nor is it to the major financial institutions. The major threat is rogue institutions, operating on a world-wide scale. Remember, VISA is everywhere you want to be.

Global operation seems to the “Mecca” for rogue activity because of the difficulties it creates for law enforcement.

I thank you for the opportunity to discuss this.

AG CORTEZ MASTO:
Thank you, Mr. Williams. Are there any questions from the advisory board?

SENATOR WIENER:
The initial identity theft legislation that I was privileged to carry, maybe two or three legislative sessions ago on behalf of this advisory board, addressed the illegality of re-encoding or forging victim information. I do not know if that would capture the issue you presented today by making it illegal to do this.

Initially, we made it illegal for someone to skim information from your card when taking it to the cash register to process your payment.

I have already requested two BDRs (Bill Draft Requests) on behalf of this advisory board. One expands the scope beyond the traditional credit and debit cards. In fact, when I was drafting the prior legislation, we initially only referred to credit cards. As we processed the bill, we added debit cards to the bill.

Is this issue about pre-paid cards that you presented here today something that we could bring in to the bill that I am already carrying forward in the upcoming session? We are looking at additional and new financial instruments that we did not know about previously.

AG CORTEZ MASTO:
I think that is possible. The more we flush it out and talk about it, I do not see how we could not address this.

SENATOR WIENER:
Mr. Earl and I have already been talking and I asked him to talk with a member of the Legislative staff, Rene Yeckley. Certainly, with permission of the panel, I would be more than happy to integrate this if it is appropriate subject matter for the bill we are already developing.

MR. WILLIAMS:
I would like to take this opportunity to extend an invitation. We would be privileged to have you come to our offices right on Warm Springs Drive. We would love to show you how this works. Touch it and feel it and see it at a much more macro level. Then we could get into the micro levels that we have seen today.

We share this with federal law enforcement when they fly in to meet with us. We have also worked with law enforcement locally to give a "Card 101" course.

The technology is moving toward an "any payment" approach. Even cell phones have technology that can be enabled to conduct credit or cash transactions. I think Mr. Earl is equally qualified to address this question. The methodology is migrating to "any platform" which would probably be a more appropriate way for a bill to address the problem.

AG CORTEZ MASTO:
Are there any further questions or comments from advisory board members in the south regarding Mr. Williams' presentation?

SAC MARTINEZ:
In allowing a law enforcement officer to use this program "on the fly", are there bank secrecy acts or other legal considerations that would limit the type of inquiry without process?

For instance, if this application was available on the scene of an arrest where the officer had a card just pulled out of the pocket of someone but it was not listed specifically in a search warrant, would there be any limitations on the law enforcement officer being able to obtain the bank related information including the amount held on the card?

MR. WILLIAMS:
Let me first state that I am not a lawyer, I want to establish that minor detail at this moment. I do not speak from a legal perspective.

I can only tell you that when I presented in South Carolina at the Advocacy Center to a room full of US Attorneys, no one brought that up as an issue. I made this presentation perhaps two or three months ago. Actually, the US Attorney here in Las Vegas has been to our office. This question was not brought up. It was suggested that the warrant should include "any debit cards or any payment vehicles".

However I have not had anyone specifically address that question to me, and I have made presentations to a significant number of lawyers.

AG CORTEZ MASTO:
Actually, SAC Martinez, I am glad you brought this question up because that was one of the first questions I had about this program.

It seems to me that these cards and related mobile devices are considered "cash". The question is whether or not there is a privacy issue when you pull someone over and you have the ability to look at that information on a card or device or not.

Conrad, do you have any thoughts on this issue? For the record, Conrad Hafen is the Chief of my Criminal Division.

CHIEF DAG HAFEN:
I have never come across any cases that deal with specifically with this issue, but I have come across cases that deal with the issue of the searches related to an arrest when it relates to a cell phone. The courts across the board, particularly at the federal level, have indicated that where there is a search incident to an arrest, the officer can go into that cell phone and glean information.

So by analogy, I would think that you could probably go in and glean the financial information off of the pre-paid card. At least that is the argument that I would make if an officer did that.

AG CORTEZ MASTO:
One final thing, Mr. Williams, you talked a little bit about being able to access the account and then "freeze" the funds before we take anything. Legally, would we have to get a warrant before we are even able to freeze the funds to put them on hold? I would assume that our intent would be to try and hold the funds for a period of time so that we can get to court to try to get the warrant to get the funds for forfeiture.

I think this is another issue that has come up as well. Would we have that ability once we have the debit or pre-paid cards in hand and we know they are the subject of criminal activity? At the time we go in and we access those accounts, can we put them on freeze without a warrant before moving forward to forfeit those funds?

CHIEF DAG HAFEN:
What is the context? Are we talking about executing a search warrant where we are going into someone's home or are we arresting somebody pursuant to a traffic stop?

AG CORTEZ MASTO:
No, the thought is you arrest somebody engaged in criminal activity and instead of a briefcase full of cash they have pre-paid cards. An officer takes that card, as Metro has done hundreds of times, and the officer then uses the contact information that is encoded on the card to find out how much money is on the card and what bank it is connected to.

Can the officer take that money immediately and transfer it somewhere, or does the officer have to freeze it and then get a warrant? To what extent is that considered private information? Is a warrant required to be able to do anything with the funds that are found on that pre-paid card?

CHIEF DAG HAFEN:
You know, I would probably advise the officers to take the more conservative approach. They may want to get a seizure warrant because they have probably cause to believe that money was connected to some criminal activity. You can get one relatively easy and quickly and get that executed and then serve it on the bank and get that money seized or frozen so it could not be transferred.

I would probably lean toward advising them in that scenario to get a seizure warrant from a judge.

MR. EARL:
Madam Chair, if I may address this issue.

In listening to this discussion, one of the questions I have is whether the procedure or the problem that you just described might be best categorized as some type of action by law enforcement in exigent circumstances. I do not know the state of law in Nevada on this nor am I up to date on the federal law either.

However my recollection is that there is an ability for a law enforcement officer to take immediate action to do an exigent search when it appears that the subject of that search might disappear or be moved expeditiously out of the jurisdiction. The theory of an exigent search would possibly be

available here, particularly if funds could be moved from a card electronically before there could be time for an application for a search warrant.

One of the factual questions that we might want to ask Mr. Williams is the speed with which or circumstances in which a criminal organization might transfer funds out of the jurisdiction or off of the card or out of the bank account that the card is associated with and whether that is likely to occur between the time that an arresting officer makes an arrest and the time that, even though it might be relatively short, an application could be made for a search warrant.

MR. WILLIAMS:
It only takes five seconds if you let the bad guy get to a cell phone and the money is gone. It is that fast. I am not here to speak to the legality issues. The practical reality of this and the way it works is that you can expect those funds would be moved immediately.

When we say "seize" or 'freeze' funds, the money has not moved. It is still sitting at the financial institution that is the issuer of the card involved. The bad guy can not access those funds by any means. It is locked up. Money has not moved on a "freeze".

I can give you ten business days to hold that transaction. It looks like a transaction that is made at a hotel on a debit card where money is 'seized'.

So I am holding 100 percent. The first thing I have to do is the balance inquiry on the card so I know the exact amount to freeze. For example with ICE, they just "seize" funds. Every agency has a different mind set.

However, if you even let the bad guy touch his cell phone, with only three key strokes the money is gone in seconds. I would love to have you come to my office so that I can show you how this is done. With only three keystrokes I can move all of the money that is on a card or cards to a bank account off-shore or where ever I want. I hope this explanation answers Mr. Earl's question.

AG CORTEZ MASTO:
Thank you. Are there any further questions from advisory board members on this subject?

MR. UFFELMAN:
Visa can probably explain this point in detail. The difference between the "freeze" we are talking about and the "seize" associated with a warrant or some other legal process is, in fact, the same process used in any other fraudulent activity.

I encountered an example of this last Tuesday during our six-day bankers' convention. I had to make arrangements to provide busses. Because I had no signature on file, money was not allowed to move from my bank to the transportation company until I personally authorized the transfer. The bank called me at my office, not at my cell phone, so, as a result, the money sat "frozen" for 24 hours. After that, it was unfrozen when I authorized release of the funds.

The procedure under discussion is much the same. There is no personal privacy issue. There are exigent circumstances because it would be real easy to move money out of an account. In any other case where fraudulent activity is suspected, Visa, MasterCard, or any other institution will attempt to contact you. In the mean time, the money just sits. As was said, there are 10 days to settle.

There is time to examine the circumstances. If a $5 card is involved, nobody cares. But, if I have five thousand $5 cards, I have real money at issue. So, a "freeze" does give you time to develop a case when an officer has found a briefcase full of cards or hotel keys – keys that have nothing to do with hotel rooms but everything to do with money transfers. If an officer has a scanner, he is then able to use the existing process.

CHIEF DAG HAFEN:
Madame Chair, I would like to make one point of clarification. Mr. Earl makes a great point when he talks about exigent circumstances but you have to realize that in order for exigent circumstances to apply you also need probable cause.

For example, if you had a situation where you had a task force member who was targeting an individual and conducting surveillance and they pulled him over pursuant to a traffic stop. If they had probable cause to believe that he was going to transfer the money or he had money that was tied in to some type of criminal activity, then they could under exigent circumstances go ahead and take that money out of the bank account.

However, in a situation where you have just a regular patrol officer who stopped somebody and he does not know this individual and he does not know he is involved in any other type of criminal conduct, he would not have probable cause to justify the exigent circumstance of going in and taking the money from the card or cards.

Therefore, it needs to be understood that distinction when we talk about such investigations.

AG CORTEZ MASTO:
Thank you.

LT. KUZANEK:
Madame Chair, may I please add a point to this discussion? This really brings up a major training issue for law enforcement.

Short of having that probable cause, it still might be a good operational procedure to allow an officer who has stopped someone for another reason and discovered those cards during investigation and has concern the person may have access to a cell phone at the point of arrest to have ability to freeze those funds on any cards on the scene.

People will say they have to make a call to someone for one thing or another. However, they could actually be moving funds involved in the alleged crime. There is that myth that everybody gets that one call after arrest. To me this is something that we need to be able to do, freeze the funds, and we need to get the word out to people who work in this area about this.

As these cards continue to become more prolific, that is going to become a much bigger concern for law enforcement. Whether it be the briefcase with 5,000 cards with five dollars on each or the one card that has a $2 million balance on it, with a couple of pushes on a cell phone button you could really be in trouble trying to piece together a financial case.

AG CORTEZ MASTO:
Thank you. Are there any additional comments or questions from the advisory board in the north?

MR. EARL:
I have one other issue, Madame Chair. So far we have talked about the holder of the card doing something or taking some action that would result in the funds disappearing beyond the reach of law enforcement.

I would like to direct a question to Mr. Williams. Are there scenarios that we might essentially term ‘fail-safe’ scenarios? This would be a scenario where a person who physically has the card does not initiate the action, however, another member of his criminal gang might take action to remove the funds from the account if he has not heard from the individual who has been apprehended with the card within a certain time frame.

Is this something that is technically possible and that you have seen in your association with law enforcement?

MR. WILLIAMS:
Yes, Mr. Earl, we do know that criminals do have “fail-safe” or “panic button” plans. If they have not heard from someone in a certain period of time, they automatically go in and move money from the cards involved. This can be done because you can access one account from multiple cell phones.

So not to hear from somebody in a criminal operation in a certain time frame or know that they have been incarcerated could easily result in a trigger to move the funds from the cards to wherever needed. Time is of the essence because of the technology involved.

MR. EARL:
So just to be clear on this for example, if I am participating in a major drug sale and I am buying the drugs. I am controlling the money in this particular drug sale. I set up a time and a place for the drug sale to transpire. Is it possible, if I understand this right, that the people I work for, if they do not hear from me by three o’clock (3:00 pm) in the afternoon and the drug deal is set for two-thirty (2:30 pm) then they can electronically take action to remove the funds from the card that would be traded by me for the illegal drugs? Is that essentially what you are saying?

MR. WILLIAMS:
Yes sir, and you can do that from anywhere in the world.

MR. EARL:
Does that also feed in to what would become an exigent circumstance? If that type of transaction is possible when you are dealing with very sophisticated drug dealers or other very sophisticated criminal gangs or terrorist organizations then that places the concept of exigent circumstance in a different context.

What I mean is that the law enforcement arresting officer might be able to lock down and control the actions of the person in front of him but still the funds could be removed because the arrangement of the criminal gang is that if one criminal failed to call in by a particular time their assumption would be that if he was apprehended, the funds would disappear.

Coming back to one of the questions that I think Senator Weiner imposed early on and that is modifications of the Bill Draft Request (BDR) that she had volunteered to take on behalf of this advisory board.

AG CORTEZ MASTO:
Actually, Mr. Earl, can I ask you to stop right there please? I want to give Mr. Majka an opportunity to speak as well with respect to this agenda item. After that happens we can come back to the general discussion if that is alright?

MR. EARL:
Surely it is.

AG CORTEZ MASTO:
That is great, Mr. Earl. Thank you. Mr. Majka, you may begin your presentation at this time.

MR. MAJKA:
Thank you, Madame Chair. I will just add a few things to the presentation this morning. I will start off with the payment card landscape that we are seeing and how pre-paid cards are part of the fraud landscape.

Most of situations that my team deals with are computer intrusions such as data breaches that you read about almost every day, primarily, where debit card or credit card data is stolen out of banks, financial institutions or from merchants and processors.

What we are seeing from a criminal standpoint is that the criminals are using the data that is being stolen, the credit card or debit card numbers, to re-encode counterfeit cards and other types of plastic and then purchase the pre-paid gift cards. They are going into Wal-Mart or other stores and they are buying volumes of these cards.

They are doing this for a number of reasons from what we can tell. They may be doing this to resell the pre-paid cards out on market for a percentage. They are also going to sell them out and people are going to make purchases with those cards.

The majority of the cards that they are purchasing do not allow them to get cash. These are gift cards that they can only use for purchases.

The other thing we are seeing is that the criminals are interested in getting these cards. Once they make that purchase and they get the merchandise, they still have the card in their possession. The card can be re-encoded as Mr. Williams mentioned earlier.

So now, instead of having to go out to counterfeit and manufacture more plastic cards, they now have legitimate plastic, whether it is VISA, MasterCard, AMEX (American Express) and Discover. They only have to re-encode the magnetic stripe on the back of these legitimate cards.

This is really what we are seeing at VISA. One of the key points from a law enforcement perspective as it relates to seizing or freezing funds is to be able to identify what is on the magnetic stripe on the cards that are seized and to quickly identify what bank the data belongs to.

VISA can work with law enforcement. We have online services for law enforcement where they can look up the BIN number as previously mentioned, to identify what bank issued that particular pre-paid card. Our service will also provide the contact information for that institution so that law enforcement can deal directly with that bank.

If they have an investigation underway, this allows them to contact the financial institution that has issued the card and explain to the investigation additional information.

Based on the belief that a criminal activity may be involved with a card, we will freeze the funds while you are getting any necessary court orders.

The other thing that I think is very important to note from a money laundering stand point is these pre-paid gift cards cannot be reloaded and have a typical limit of about $750. So you will not see a lot of large purchases on gift cards. It has been shown that a typical average load on a pre-paid gift card is actually about $65.

Again, I just want to emphasize the fact that we work with law enforcement on a regular basis which includes the FBI, the Secret Service, the U.S. Postal Inspection Service and local law enforcement agencies.

We can provide them with training if necessary. We can provide them with a magnetic stripe reader for the Las Vegas area so that they can swipe the card and identify what is on that magnetic stripe. From a criminal prosecution stand point, it is very important that they know there may be something different on that magnetic stripe then what is on the card’s face. Quite often that will be different.

Other than that, most of our unit handles data intrusion and we are seeing in the pre-paid space that the criminals are getting more active. They are trying different techniques with the pre-paid cards. You may have heard of a lot of arrests where the criminals have pre-paid cards in their possession and there have been a number of groups involved with this activity.

From our stand point, we are primarily seeing the criminals are reselling the cards on the 'black market'. They are selling them off to gangs who are out and making purchases of merchandise and then they are re-encoding the same cards for additional spending schemes.

AG CORTEZ MASTO:
Thank you, Mr. Majka. Let us start in the north this time. Are there any questions from advisory board members in the north for Mr. Majka?

MR. EARL:
Madame Attorney General, if I may, I would like to follow up on the question that I think both you and Senator Wiener talked a little bit about and that is the possibility of personal information being contained on the magnetic data.

Personal information has a very specific statutory meaning in Nevada. I will not read the whole definition but it seems to revolve around whether an actual person's first name or initial and last name appears in conjunction with certain other data like a Social Security Number or a driver's license number.

I think I understood from Mr. Williams that in a legitimate pre-paid card or gift card or whatever one calls it, the magnetic data would not contain a person's name or social security number or that type of personal information. I would just like to confirm that because that probably takes the issue out of the Nevada law dealing with personal information and any possibility that a pre-paid debit card would obtain personal information.

If I can I get a read on that issue from Mr. Williams and Mr. Majka that would be terrific.

MR. WILLIAMS:
There are two kinds of pre-paid debit cards. There are anonymous cards and in the anonymous world there is no information on the magnetic stripe or in a database.

For example in the world of payroll cards, a name is generally encoded on what they call "track one" so you will see on the magnetic stripe that there are two primary tracks that are used. Mostly there are numbers that are embedded with security algorithms that I need to authenticate the transaction.

For example, we would normally embed in the "track one" the individual's name. So you would see what is shown on a credit card receipt that you sign.

The credit card device is lifting that off of the magnetic stripe. After that there is no data that is personally identifiable on a magnetic stripe. This would only be relevant to high value payroll cards which function more like a credit card. Does that answer your question, Mr. Earl?

MR. EARL:
Yes it does, thank you.

MR. WILLIAMS:
Just to add an aside here, law enforcement sees the anonymous cards far more often then they do the personalized cards.

AG CORTEZ MASTO:
Thank you, Mr. Williams. Are there any other comments or questions from members in the north? Members in the south, are there any further comments and questions on this agenda item?

Gentlemen, thank you very much for your very informative presentations. We appreciate you being here today.

We will now move on to the next Agenda Item.

Agenda Item 8 – Overview of plans, strategies and coordination regarding mortgage and foreclosure fraud.

AG CORTEZ MASTO:
I believe Mr. Earl may have put this on the agenda to inform advisory board members of the good working relationship that exists between the state, local level and federal authorities in the area of the mortgage fraud crisis that we have here in Nevada.

There is a lot of this type of fraud going on here and this includes foreclosure rescue scams. Not only do we have at the state level a strike force working on those fraudulent activities but, there is a strike force at the local and federal levels working on these issues. We all work very well together. We are sharing our resources so we are not duplicating our efforts.

From my perspective, I want to thank those local and federal authorities for coming to the table and working so well with all of us. Thank you for those efforts.

I am not sure if anybody else has any comments with respect to this topic. If you do, go right ahead at this time.

SAC MARTINEZ:
Thank you, Madam Chair. I can give a quick overview of what has occurred here since early this year.

Back in the January to February time frame, my supervisor Scott Hunter who has the "white collar crime squad," had already put a working group together to look at the mortgage fraud issue here, especially in southern Nevada. We started to reach out to some of our counterparts who are stakeholders in the federal government and in the state and local governments.

On March 13, we made an official announcement jointly with U.S. Attorney Greg Brower announcing the existence of our mortgage fraud task force. It involves participation with the FBI. I have four full time agents assigned to it and they are joined by agents from Las Vegas Metro, the Office of the Attorney General, the Social Security Administration's Office of Inspector General (OIG), the United States Postal Inspection Service, the United States Housing and Urban Development OIG, the U.S. Attorney's Office for prosecution support, the Internal Revenue Service criminal investigations branch and the United States Secret Service which has recently come on board.

We discovered by reviewing the rising foreclosure rates that we had some major mortgage fraud issues to look at. To date, 32 active mortgage fraud investigations are being conducted by the task force.

Today we can attribute to task force efforts four indictments, six "informations" that have been done in federal court and we anticipate some additional indictments coming within the next week.

In a broader context, this is something that has been very much the focus the FBI nationwide. The criminal investigative division of the FBI has an initiative that we are calling the "operation malicious mortgage" arm.

The task force really dovetails right into our national level efforts. There will be a joint press conference at the end of next week involving the FBI and the Department of Justice in which we will be talking some of the nationwide statistics related to the efforts that have occurred. There have been task forces that have stood up all across the country in the major cities that are affected by this problem.

So again, as you mentioned, Madam Chair, I just wanted to give a quick overview of some of the efforts that are occurring and the way that we go about this – leveraging everyone's expertise and addressing what is a real emerging crime problem here.

When we kicked off the task force in that press conference, we did mention that there is a hotline number. I will read that now for the Southern Nevada Mortgage Fraud Task Force. The number is 702-584-5555.

To date, we have received 507 hotlline calls. We have a team that does the triage work for the complaint calls that come in either over the hotline or as walk-in complaints from someone who may bring these types of things to our attention.

There is a lot of work going on to try to examine those cases and to decide where the best place is to handle them, especially considering possible aggregations so that losses will meet thresholds for federal prosecutions.

AG CORTEZ MASTO:
Thank you, SAC Martinez.

For informational purposes, we are also working with the victims themselves, the individuals who unfortunately find themselves in a default situation.

Nevada Treasurer Kate Marshall, United States Senator Harry Reid and my office have organized and are hosting foreclosure prevention seminars. One is occurring right now at Cashmen Field today until 7:00 pm and tomorrow from 10:00 am to 5:00 pm.

We are doing this with the help of lenders in this community and in this state. There are 20 lenders coming to the table with those individuals who have the potential of being in default. They will be able to sit down and try to explore renegotiating the terms of their mortgage or working out an arrangements with them to keep them in their homes longer. Hopefully, they can come to some sort of agreement with respect to staying in their homes and receiving counseling on their financial situation.

So not only do we have lenders assisting us with these seminars, but we also have counseling services that are going to be there. Members of my office and other offices throughout the state will work with these individuals on whatever level they may need to try to keep their homes.

We will also be in the northern part of the state in the coming weeks to make sure we are reaching out to all individuals who may be facing these mortgage issues. We will be announcing those dates as we move forward.

Are there any further comments about this subject from advisory board members?

SENATOR WIENER:
I know Ms. Pierce is doing the same thing as I am. We are walking out in the neighborhoods. I have done 15 major walks. As I have done my walks, I have found one out of six or seven houses is for sale and I don't get to talk with the residents because they are not there.

However, there is an issue that has come forward through calls I have received and in face to face conversations that I have. In fact, I just recently had a call from a woman regarding a "renting to own with the intent to own" scheme. She has put about $13,000. in payments on the house but the person from whom she renting to own from is now being foreclosed upon. Also there are people who rent apartments where the owner of the building is in foreclosure.

Do we have some kind of renter protection that we are going to be addressing for the people who are truly victimized? In good faith, they stayed current with their "rent to own" agreement with the homeowner or building owner, but that owner did not stay current on the underlying property loan

AG CORTEZ MASTO:
Senator Wiener, I can address that from the complaints that we see coming in to my office locally and I am sure SAC Martinez has seen the same complaints. That problem, unfortunately, gets tied in to this fraudulent activity.

Those situations fall under what we call "foreclosure rescue scams". Someone will know that a house is in foreclosure. They will contact those individuals and usually the scheme goes like this – I will give you $500. cash and you sign your deed over to me and we will work through this and help you save your home. In the meantime, they will turn around and rent that house to some unsuspecting tenant who will come and make payments to rent the home for a six month to an eight month period. The new renter then learns that the house goes into foreclosure and they are out of their rent money.

We have complaints like that coming in. Part of our process to deal with this is the prevention and education component for prevention. We are getting out into the community and making people aware of what is going on and letting them know if they are looking to rent a home that they can contact my office. We will put them in contact with the appropriate individuals to do the background check on those homes and make sure that before they rent a home that it is not in foreclosure. That is easy enough to do.

SENATOR WIENER:
Again, that is part of reaching the person that is here and is part of the economic downturn. There is also the person who does not even get into the home but goes into the rental property or apartment and that building is in foreclosure but the renter does not know to ask that question because they do not suspect that the home they are preparing to rent may be in foreclosure.

Is there a number you mentioned at your office, Attorney General, or the one mentioned with the Task Force that I can use to tell people to call when I am talking to them at the door or when they call me?

SAC MARTINEZ:
You absolutely can give them the number I gave out earlier and if it turns out to be more of a matter of victim services, we will then refer them to the appropriate victim support services.

AG CORTEZ MASTO:
Along with giving them the Task Force phone number that SAC Martinez gave us today, you can also have people call my office and we will put them in touch with the appropriate victim counseling services.

That is one of the reasons for these weekend seminars that we are doing. It is not just for those individuals that are already in foreclosure with their homes. This is also for those individuals who may have an ARM (Adjusted Rate Mortgage) that is coming up for reset and they are concerned. Those people can come to these seminars we are hosting. We also want to reach individuals you describe who have renting issues related to foreclosure. There will be counseling services at the seminars. We can put them in contact with the appropriate help.

On my website, the Nevada Attorney General's website (http://ag.state.nv.us/) there is additional information available as well.

SENATOR WIENER:
I understand that if someone is thinking about renting a house and are concerned about the status of the house, they can call your office and find out if it is in foreclosure?

AG CORTEZ MASTO:
They can contact my office and we will help them find that information or refer that to the appropriate agency that can help them find that information.

SENATOR WIENER:
That is very good. Thank you, Attorney General Masto.

AG CORTEZ MASTO:
Are there any further comments with respect to Agenda Item 8? Hearing no further comments, we will move on to Agenda Item 9, Mr. Earl.

Agenda Item 9 – Legislative Issues Update.

MR. EARL:
Madam Chair, this is a brief report on issues that have previously been before the board on a substantive basis.

First, the board has previously dealt with issues regarding obtaining information from Internet Service Providers (ISPs) and other telecommunications service providers. This relates to a BDR that will be put forward by the Attorney General and I am coordinating internally with the Attorney General's staff relating to that particular BDR.

Turning to the BDRs that Senator Wiener is going to carry on the board's behalf, there are two as she mentioned. I have been in touch with the Legislative Counsel Bureau (LCB) attorneys, first with regard to the statutory requirement that businesses encrypt electronic transmissions containing personal information. We are awaiting some private sector information with regards to that.

The second BDR which Senator Wiener referred to under a previous agenda item deals with updating certain criminal provisions relating to debit and credit cards. We have gone through a process that has involved representatives from Las Vegas Metropolitan Police and Mr. Hafen to produce a current draft of changes in the statutory text. One of the things that I anticipate working with both Mr. Hafen and Metro officers and others including Mr. Williams is any additional changes in the draft that might be appropriate.

That is all I have, Madam Chair.

AG CORTEZ MASTO:
Thank you very much. Are there any comments? Hearing none, we will move on to Agenda Item 10, Board Comments.

Agenda Item 10 – Board Comments.

AG CORTEZ MASTO:
Are there any advisory board members who wish to make any comments at this time?

SAC MARTINEZ:
Yes and my comment is particularly for your edification, Jim. I wanted you to know that Supervisor Eric Vandersteldt is tuned in to this board meeting over webcast. He is on leave this week and is in California. He is hearing this loud and clear. I want to let all of you know that we have an audience of at least one.

AG CORTEZ MASTO:
That is great. Are there any other comments from advisory board members? Hearing none, we will now move on to Agenda Item 11.

Agenda Item 11 – Public Comments.

AG CORTEZ MASTO:
The Public Comment period is an opportunity for members of the public to address the advisory board. I do not see any members of the public here in the south. Are there any members of the public in the north who would like to address the advisory board?

MR. EARL:
No ma'am.

AG CORTEZ MASTO:
Thank you. Moving back now to Agenda Item 10 under Board Comments, Senator Wiener, do you have a comment to make at this time?

SENATOR WIENER:
Thank you, Madam Chair. Ordinarily, do we look at the next meeting date at this time on the agenda?

MR. EARL:
I think we have a meeting date that has already been cleared and scheduled but I can not recall it.

MR. UFFELMAN:
September 25 is what I have written in ink in my calendar so it must have meant we discussed it.

SENATOR WIENER:
Okay, I have that date. Thank you.

AG CORTEZ MASTO:
Thank you.

Agenda Item 12 – Adjournment.

AG CORTEZ MASTO:

Motion to was made by Mr. Uffelman and seconded by Senator Wiener.

Motion to approve adjournment passed unanimously.

Meeting adjourned at 11:23:39 AM.

Respectfully submitted,

_Ursula K. Sindlinger____
Board Secretary

Approved by the Board at its subsequent meeting on September 5, 2008.

Minutes of the
Nevada Technological Crime Advisory Board

September 5, 2008

The Nevada Technological Crime Advisory Board was called to order at 10:00 a.m. on Friday, September 5, 2008. Attorney General Catherine Cortez Masto, Chair, presided in Room 3138 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada. The meeting was webcast.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Nevada State Senator Valerie Wiener (Advisory Board Vice-Chair)
Gregory Brower, U.S. Attorney, Department of Justice (DOJ)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Chris Ipsen *(Rep. for Dan Stockwell, Director, NV Dept. of Information Technology)*
Sheriff Mike Haley, Washoe County Sheriff's Office
Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)
Dale Norton, Nye County School District Assistant Superintendent
Nevada State Assemblywoman Peggy Pierce
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Special Agent Melissa McDonald, *(Rep. for Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE))*

ADVISORY BOARD MEMBERS ABSENT:

Tray Abney, Reno/Sparks Chamber of Commerce
Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)

TASK FORCE MEMBERS PRESENT:

Detective Dennis Carry, Washoe County Sheriff's Office
Lieutenant Bob Sebby, Las Vegas Metropolitan Police Department
Supervisory Special Agent Eric Vanderstelt

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director
Conrad Hafen, Nevada Chief Deputy Attorney General, Advisory Board Counsel

OTHERS PRESENT:

Lt. Charles Cohen, Indiana State Police
Marshall Emerson, Washoe County Sheriff's Office
Kathy Fox, Washoe County Human Resources
Lea Lipscomb, Retailers Association of Nevada
Keith Munro, Nevada Assistant Attorney General
Todd Shipley, Vere Software
Tracy Woods, Retailers Association of Nevada

Agenda Item 1 – Call to Order - Verification of quorum

AG CORTEZ MASTO:
This meeting is called to order on September 5 at 10:00 AM.

A roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Discussion and approval of minutes from June, 2008 Advisory Board Meeting. (Discussion/Action Item)

Motion to approve the minutes was made by Senator Wiener and seconded by Assemblywoman Pierce.

Motion to approve minutes passed unanimously.

Agenda Item 3 – Future action upon resignation of the Board Secretary. (Discussion/Non-Action Item)

AG CORTEZ MASTO:
This item is to discuss future action by the advisory board following the resignation of our board's secretary. This is not a negative thing as she has moved into another position within the Attorney General's Office. Jim, would you like talk a bit about this discussion item?

MR. EARL:
This is the second board secretary that has left during my tenure here with the Tech Crime Advisory Board.

During the last replacement action that we had, I delayed filling that position for a number of months in order to reprogram funds. I am not sure that will be a viable option this time.

When the last vacancy occurred, I undertook a recruitment drive that took place immediately after the close of the Legislative session. This enabled me to attract 59 applicants, many of whom were very well qualified in terms of taking meeting minutes that meet the Legislature's standards.

When we last filled the position the advisory board gave me the authority to write a job description, check it with senior staff at the Attorney General's Office and then post it for public response. The advisory board requested that I bring the three top candidates to them for consideration after I conducted an informal interview process.

I am willing to do that again or the board could delegate the ability to hire to me or to the Chair or some other combination. This decision does not necessarily have to be made at this meeting. As a matter of fact I am perfectly open to having this position to remain open for awhile.

However I do think this is something the board should think about what the process should be.

AG CORTEZ MASTO:
Is there any further discussion on this agenda item?

MR. UFFELMAN:
I think the process that Jim has described reflects the old days of this advisory board. Under Jim's guidance, the board operates quite a bit differently now. I am comfortable with Jim doing the interviewing process and perhaps with the Chair having final approval of his selection. This would speed things up and make it work. This is someone who will be working with Jim and not necessarily with every advisory board member.

AG CORTEZ MASTO:
Is there any further discussion?

SHERIFF HALEY:
I support what was just proposed.

AG CORTEZ MASTO:
Is that in form of a motion?

SHERIFF HALEY:
It's not an action item on the agenda.

AG CORTEZ MASTO:
That is correct. Thank you very much, Sheriff Haley.

SAC MARTINEZ:
Madam Chair, I have a question for Jim.

In the past, Jim, when you were looking for some forensic expertise you put a committee together to help out. If you would like to populate a similar committee to conduct interviews, we would be available to participate in that.

MR. EARL:
Thank you very much for the offer, SAC Martinez. I do not want to make a decision on that detail right now. This position, although we would like to have it be quite skilled, does not necessarily involve the same set of forensic skills as were required for the computer forensic examiner positions.

It would involve somebody who would have the ability to produce meeting minutes from a recording; conduct Internet research on a wide variety of Internet and technology topics, and would have the ability to run financial planning software. The person also would interface a wide variety of individuals.

Once again, I thank you for the offer and I will take it under consideration.

AG CORTEZ MASTO:
Is there anything further to add to this discussion? Hearing none we move on to the next agenda item.

Agenda Item 4 – Report regarding Task Force Activities. (Discussion/Non-Action Item)

AG CORTEZ MASTO:
Who would like to start with reporting on task force activities from the south?

SAC MARTINEZ:
Madam Chair, I would like to invite Supervisory Special Agent Eric Vanderstelt to represent the cybercrime task force here in the south and give a quick synopsis of some of their activities since our last meeting.

AG CORTEZ MASTO:
Thank you.

SSA VANDERSTELDT:
Thank you, Madam Chair and board members. I appreciate this opportunity to talk about some of the activities the task force has been involved with since your last meeting. I have a few cases to go over with you that represent our recent activities.

On April 18, 2008 a man was convicted on one count of interstate transportation of child pornography and one count of possession of child pornography. The case was initiated when the man was stopped by the Wyoming Highway Patrol for a traffic violation. Computer hard drives in the vehicle were determined to contain thousands of images of child pornography.

On July 18, the man was sentenced in the District of Wyoming to 18 years to 15 years of incarceration. The man was a resident of local chapter of the Hell's Angels Motorcycle Club and owner of a local area brothel.

This case was investigated jointly with the Wyoming Highway Patrol and the Reno Police Department.

On June 6, 2008 a man was found guilty of one count travel with the intent to engage in a sexual act with a minor and one count of coercion and enticement of a minor. He had communicated with a 14-year old female in an Internet Relay Chat (IRC) room and then traveled from southern California to Las Vegas with the intent to engage in a sex act.

He had utilized a Personal Digital Assistant (PDA) for communication which was found on his person at the time of his arrest. A forensic examination found stories concerning sex with children. He was sentenced to five years in federal prison.

On July 2, 2008 a man was sentenced to ten years of custody and lifetime supervision after having pled guilty to one count of coercion and enticement of a minor. He had repeatedly requested to engage in various sex acts with a 14-year old female on MySpace and then attempted to meet with her.

On August 5, 2008 a man was sentenced to serve 70 months in federal prison and ordered to pay $370,819. restitution. He had used stolen personal identification information and fraudulently obtained debit and credit cards to finance a lavish lifestyle. He had pleaded guilty earlier to access device fraud, identity fraud, possession of equipment used to produce false identification documents, and aggravated identity theft.

This was interesting in the sense that the man had hacked into PayPal accounts and obtained debit cards and used them at local businesses. The investigation also revealed that he was using false identities and fraudulent cards for medical treatment, to purchase real estate, secure a mortgage, and to make his house payments. He also used false identities and fraudulent cards to obtain computer equipment and to lease expensive cars.

His actions resulted in a loss to American Express, PayPal and others in the range of hundreds of thousands of dollars. The search recovered identification document making equipment, credit card numbers, American Express merchant terminals, old credit reports, and an extensive amount of computer equipment.

Forensic analysis of the computer equipment revealed stolen identity packets, false identification documents bearing the defendant's and other individual's photographs, encryption software, encrypted files, codes to encrypt the files, computer hacking software, and software that is used to hide the identity of the computer while on the Internet.

These are a few cases that I selected to share with the advisory board that are representative of type of work the task force has been engaged in since your last meeting. Thank you for your time.

AG CORTEZ MASTO:
Thank you, SSA Vandersteldt. Are there any comments or questions about this report?

SHERIFF HALEY:
I have a quick question. Do you have a whole army of people that are helping you do this work?

SHERIFF GILLESPIE:
I will answer that but could you clarify your definition of "army"?

SHERIFF HALEY:
I forgot you were there, Sheriff Gillespie. Let me rephrase my question. The point I want to make is that the amount of work you have done on these cases requires a lot of people to investigate just one of these of cases. Putting it into a package for court requires another army of people and we simply do not have the necessary number of people or resources available in the north.

So, my question is how many people are working in your operation on these particular cases?

SSA VANDERSTELDT:
In answer to your question, the Federal Bureau of Investigations (FBI) has 12 agents assigned to work cyber investigations matters. We are joined by the component of Las Vegas Metropolitan Police Department (LVMPD) that deals with Internet Crimes Against Children (ICAC) and their fraud unit and property crimes detail. So when we work jointly together we are able to multiply the force here and achieve results such as the ones I presented today.

SHERIFF HALEY:
So it is only through that multiplication of resources that you are able to stay in the running with these results?

SSA VANDERSTELDT:
That is correct. The investment of time into these cases is quite significant and the only way we can achieve the type of results that we have is through cooperation with other agencies. I hope this answers your question.

SHERIFF HALEY:
Great, and thank you very much.

AG CORTEZ MASTO:
Thank you. Are there any other comments or questions? Are there any reports of the task force in the north?

SHERIFF GILLESPIE:
Madam Chair, I would like to ask Lieutenant Bob Sebby from Las Vegas Metro to come forward and maybe touch a little bit on Sheriff Haley's question with regards to some resources that we have committed to these efforts as well. Lt. Sebby gave me a briefing a few days ago on some newer technologies and trends we are seeing down here in the valley that we would like to share with the board.

AG CORTEZ MASTO:
Thank you, Sheriff Gillespie. Please make your presentation, Lt. Sebby.

LT. SEBBY:
Thank you. My name is Bob Sebby and I am a Lieutenant with Las Vegas Metro's Financial Crime Unit. It is only through cooperation with the FBI, Secret Service and all of the task forces that we have down here that we are able to get anything done.

I am still getting about a thousand cases a month. In Las Vegas is we have always had the counterfeit credit cards and debit cards scammers who come to Las Vegas in order to steal our money and take it away. The biggest trend that we are seeing right now involves the use of

skimming devices that are used to steal private information on magnetic stripes on credit, debit and prepaid cards.

We recovered four skimming machines from waiters working at high end restaurants located on the Las Vegas Strip. I also know of a skimming machine that was involved in criminal activity at a restaurant in Carson City recently. That machine should be coming back on the scene in a few months again because criminals use these in cycles.

We are also seeing a large increase in the amount of gasoline pump skimmers and the technology is becoming more advanced. These machines are wireless now.

Over the course of the last five months we have been working with investigators from American Express, CitiGroup, and Discover Card on 15 "skim" sights spread between California, Arizona, Nevada, Colorado and Utah. This is what we are up against with this type of criminal activity.

Northern Nevada will also start to experience an increase of these "skimmers" in casinos and restaurants. Tourists are the prime victims of this criminal activity in most locations but locals are targeted as well. In our economy, we must take this threat extremely serious.

AG CORTEZ MASTO:
Thank you, Lt. Sebby. Are there any comments or questions from the board on his presentation?

SENATOR WEINER:
Madam Chair, I would like to ask a question of Lt. Sebby. I remember your presentation from an earlier meeting about the gas cards and skimmers. I frequently get calls about this problem from concerned constituents. Is this skimming activity still happening at the actual pump or they are now finding a way to skim customer financial data at the register as well?

LT. SEBBY:
We are recommending that customers go inside the gas station to pay with your credit or debit card. As long as the pin pad is on the counter and your card does leave your sight when you hand it to the clerk, you should be fine. We found one skimmer where a clerk was actually taking the customer's card and skimming by taking it under the counter where there was a skimmer connected to a laptop. That has been an isolated incident so far.

Most of the criminal activity connected to skimmers at gas station has been outside at the pump itself. That is why we are trying to do as much training as we possibly can with customers and the gas station service industry.

AG CORTEZ MASTO:
Thank you again, Lt. Sebby. Are there any additional questions on this subject?

ASSEMBLYWOMAN PEGGY PIERCE:
Lt. Sebby, what leads you to find a card skimmer at a gas pump? What tips someone off that a device is present on the pump?

LT. SEBBY:
In many situations, there is a wireless skimmer on the pump. Some officers have wireless laptops in their vehicles and we frequently drive through or past gas stations. Our laptops will pick up the wireless connections around the vehicles. If we suddenly pick up a wireless signal in the parking lot or drive-through area of a gas station, we know we may have this sort of activity going on right then and there and we investigate.

Sometimes, though, our investigations begin after the wireless theft has already occurred. However, we are working very closely with the credit card companies now. As soon as they get one complaint, we immediately contact all the rest of the companies to find out if they have

customers who have experienced from similar activity at the same gas pump. This information helps us back track and recover the skimmers.

One other point I wanted to add is that we are also seeing these skimming machines on more Automatic Transaction Machines (ATMs) that are located outdoors.

AG CORTEZ MASTO:
Thank you. Does anyone else have any questions or comments? If not, do we have any task force activity reports from the north?

SHERIFF HALEY:
We have Detective Dennis Carry in the north to speak about a recent operation.

AG CORTEZ MASTO:
Thank you again, Lt. Sebby. We will now hear from Detective Carry.

DETECTIVE CARRY:
Thank you again, Attorney General Masto. My name is Dennis Carry and I am a Detective with the Washoe County Sheriff's Office and a member of the Nevada Internet Crimes Against Children Task Force (ICAC) and the FBI's Innocent Images Task Force.

In the first few months of this year, the task force in the north served over 15 search warrants involving child pornography. In those 15 search warrants we recovered over 120,000 child pornography images and over 9,000 child pornography videos. We have arrested eight people out of the 15 search warrants so far and we expect to arrest at least 11 total.

With the work going on up here in the north, we are essentially "drowning." We need more help for what we are doing. When we serve the initial search warrants, Las Vegas Metro ICAC sends up people who can assist us, and I thank them for that. I also appreciate the assistance we get from the FBI and the Attorney General's Office. There is more work to be done if we had the resources and the manpower to do it.

Right now, the biggest backlog is in computer forensics. When we recovered 120,000 images and 9,000 videos of child pornography, we found that we had reached the point where things started to become too confusing to focus on other digital evidence we might have.

We have over 40 hard drives to analyze in a short amount of time. This is an ongoing issue. We are expecting a lot more cases in the near future.

We did do a press release recently, but we wanted to present the information to the board and let you know there is a big ongoing problem right now. The task forces throughout the state are working diligently to track these criminals down and remove these computers from being accessible to other members of the public who are downloading child pornography.

Thank you for the chance to update you on our task force efforts.

SHERIFF HALEY:
I want to follow up on what Detective Carry has just said and compare it to what is going on with the task force in the south. We really need to replicate in the north a more solid working team that works at a specific location. We have talked about that up here.

As Dennis indicates, they are buried in cases. This prevents them from digging further and it prevents them from going out after more criminals who are perpetrating these crimes. They just do not have enough personnel.

I know this issue is something that this advisory board has talked about and committed to moving forward with in a way that could help Detective Carry and other law enforcement agencies involved to do their jobs better in the north.

AG CORTEZ MASTO:
Thank you, Sheriff Haley. Are there any other comments or questions? Hearing no further comments, I thank you, Detective Carry for your presentation.

Are there any other reports from the task force in the north?

SA MCDONALD:
This is Melissa McDonald from the United States Department of Homeland Security Immigration and Customs (ICE). Thank you, Madame Chair.

In support of Sheriff Haley's comments in regards to lack of trained personnel here in the north, it has been a benefit to have some assistance from the south. ICE has stepped up as far as supporting the northern Nevada component of the cybercrime task force.

As far as specific numbers, up here we have an active number of people that includes me and two individuals from the Nevada Attorney General's Office. ICE has provided space, equipment and training for folks on the task force up here.

However, we do have additional room available and that is one thing that I see here – a lack of communication within the agencies in the north which includes both state and local offices. I think part of that is because everyone is so overwhelmed here in the north that this has been an ongoing problem.

I had the recent fortune to speak with Mr. Todd Shipley who is currently here in the audience in the north with regards to solutions to these problems. A great suggestion that came up is the possibility of establishing a local chapter here in the north of the IHTCIA, the International High Technology Crime Investigation Association. This could perhaps be a means to help initially address the communication aspect and with training.

IHTCIA is an organization that also allows civilians and governmental law enforcement agencies to participate providing they have the specific criteria to do so. This organization provides substantial training in related technology fields not offered by local governments.

We are currently formulating a plan to try and recruit enough members in our area to meet criteria of 20 members. This would allow us to form a chapter to obtain training opportunities and communication options that might help out with some of these issues that we have here in the north. Thank you, Madam Chair.

AG CORTEZ MASTO:
Thank you. I appreciate the comments and I think this is exactly why this advisory board is here. We come together to address issues such as those presented here this morning. I think there is an opportunity in the north and the south, but particularly in the north, to work through communication and resource issues and get the additional manpower that is needed.

This is something this advisory board and Mr. Earl can help us work through. Any time there is a need, this board should be working on it.

Are there any other comments or questions under this agenda item? Hearing no additional comments or questions, we move on to Agenda Item 5.

Agenda Item 5 – Presentation by Lt. Charles Cohen, Indiana State Police, Problems facing law enforcement: Inter-relationships among social networking and virtual world web sites, identity theft and related frauds, and drug and terrorism funding. (Discussion/Action Item)

AG CORTEZ MASTO:
I have the pleasure this morning to introduce our guest speaker to the board. Mr. Earl and I asked this gentleman to come and present to you. His name is Lieutenant Charles Cohen from the Indiana State Police.

Lt. Cohen, could you please come up to the presenter's table please while I introduce you to the board? I apologize that I am not down at the southern location of this meeting and able to meet you personally. We have spoken on the telephone. I thank you for coming here today to speak with our board in Nevada.

Now I will read some of your background information so the board knows who you are and why we have asked you to come and speak to us today.

Lt. Cohen is a nationally recognized cybercrime expert from the Indiana State Police and today he will be presenting on problems facing law enforcement such as interrelationships between social networking, virtual world web sites, identity theft and related frauds, and drug and terrorism funding.

Lt. Cohen has been with the Indiana State Police for 14 years and is currently the commander of special investigation in criminal intelligence sections. In this capacity, he is responsible for the cybercrime, white collar crime, vehicle crime and crimes against children units along with overseeing the department's overt and covert criminal intelligence functions. He has cross-designated as a Special Deputy United States Marshall sponsored by the Internal Revenue Service Criminal Investigations Division.

Earlier this year, Lt. Cohen was featured on the cover of Informant Magazine published by the National White Collar Crime Center (NW3C). His article outlined the importance of computer forensic triage, the basic onsite computer examination performed by investigators who aid in any initial questioning of a criminal suspect.

Some of you may not know this, but Lt. Cohen is in high demand. He is on the speakers' circuit because of his expertise and knowledge. We are very pleased and honored to have you here today, Lt. Cohen, and we are very interested to hear what you have to say.

LT COHEN:
Thank you, Madame Chair.[1]

Normally I present to law enforcement officers and enlisted people in the intelligence community. However, since I am talking to decision makers today I want to find a way to show you some of the challenges and opportunities that law enforcement people face in this area.

I will start with some case examples that I have come across in a bit more depth than some of the presenters before me today shared because some of these cases have been adjudicated and I am freer to talk about them in a way that will allow you to see what is going on.

I have to give you a quick warning disclaimer though about the topic matter, particularly because some people in the audience are not in the law enforcement community. You may see some

[1] Lieutenant Cohen's oral presentation was accompanied by a visual Power Point presentation, which contained embedded video and over 130 static slides. The static portions of his presentation are on file with the board.

naked people because people do not just go out to the Internet to just look at some bad words. I promise you all this is not done gratuitously.

If anything I say offends you, please do not blame the Indiana State Police that I represent, but I will try not to offend anyone.

The other quick disclaimer is they told me that I would only be talking two hours but I will modify that to fit everyone's comfort and physical needs as we go forward.

This is the challenge we are facing right now. There are over 300 online social networks out there. When you add in video sharing sites like YouTube, photo sharing sites like Flickr, Photo Bucket and others, it pushes the number well over 500. That is before you even begin talking about virtual worlds and the massive amount of online role playing games. There are another 100 of these out there right now and another 100 that will be released by the end of 2009. We will talk a little bit about those.

So the challenge is just the overwhelming nature of it. My guess is that no one in this room, including the experts here today, recognizes all program logos up there. That is one of the challenges. Some may not recognize any until they find MySpace on the list right up here.

This is just one of the challenges we face – the problem of the sheer volume of ways people can interact on the web today. This challenge has been around for a long time.

Let us just talk about social networking. That has been around since caveman days when caveman A went over to caveman B's cave to find food, fire or fun. That was social networking. The difference back then was it was done face to face in the same location in a well known way.

Now you add in the distance of geography, the issue of anonymity, whether intentional or unintentional on people's part, it just creates challenges for law enforcement especially when we talk about jurisdictional boundaries. It was a challenge enough for law enforcement to deal with a criminal going across county lines or state lines. Now it is very common that the victim and the suspect are not even in the same country or the same hemisphere. This creates a challenge for law enforcement.

But this has been a problem for a long time. The special agent mentioned Internet Relay Chat rooms or IRCs. That has been around since 1984, and as you heard from his statement, it is still being used by bad guys.

So basically we are now finding that "old school" ways to communicate on the Internet are not going away and we are finding more and more new ways to communicate are being added. This creates an ever increasing challenge for law enforcement.

Internet Relay Chat and UseNet have been around for awhile – UseNet since 1979. These are still are in actively used to do things like trade child pornography, and trade databases containing hundreds of thousands of stolen credit card numbers on a daily basis. These things are really going on. And as you move on through time, you find out about some of the "new school" things that have around since about 2002, like MySpace, Face Book, Bebo and Zega and the other 295 or so programs that are out there.

There are also things like Massively Multiplayer Online Role Play game, things like Dungeons and Dragons. There are also things like World of Warcraft (WoW) that have evolved from Dungeons and Dragons. They are ripe for use in criminal exploitation as I will show you a little bit later on.

All these things provide for more work and increasing challenges for law enforcement. We are taking about lawful intercepts such as Federal Title III wiretaps or state intercepts. The challenges

have gotten very difficult when you think about the possibility for someone on their web-enabled mobile phone to go from cell phone technology to internet technology to use Voice Over Internet Protocol (VoIP) on cell phones.

So your surveillance team is telling the guys in the wire room “he is on the phone now” and they are saying “we have nothing.” The criminal has logged on and roamed anonymously way to a VoIP provider that could be located in eastern Europe or the United States and is talking in a secure manner on what is called a 256-bit tunnel equipped site.

For you lay people who want to know what that is, it means it is almost impossible for even the government intelligence agencies to break into that for surveillance purposes. This is difficult for law enforcement but provides opportunities when law enforcement has training, equipment and resources to be able to address what is out there.

The last thing on this set of slides is the Multi-user Virtual Environments or Virtual Worlds. That is what the people on this committee will be faced with over the next five years – multi users interacting in virtual worlds.

Now I want to talk to you about specific cases to provide you with examples of what I have just shared. The first case is involves a victim named Taylor Behl. Some of you may have heard of her case in a town in north Virginia that received national attention when it was going on. In fact, 48 Hours actually did an hour segment on this case.

They talked about the trial and some of the investigation that had a violence and sex aspect to it. I want to talk about the online personality aspect of this case and the challenge.

Basically, Taylor was 17 years old and an incoming Virginia Commonwealth University student. It happened at this time of the year. It actually happened on Labor Day weekend. Taylor grew up in Vienna, Virginia which is about a two-hour drive from the VCU campus so she wasn’t someone who was very familiar with the campus area.

She was an active user of various online social networks including MySpace and Live Journal. For those of you not familiar with the second one, Live Journal is like all social networks, but it is going to have a lot more words and a lot less video and music and pictures than you may generally find on other social network sites.

She picked a user name for herself, “tiabliaj”, at Live Journal. I generally ask people in law enforcement if they notice anything in particular about that name. She spelled “jail bait” backwards for her user name when she set up her Live Journal account. At 17 years old in many states, including Virginia, she was in fact “jail bait”.

She disappeared at about 10:00 at night. That was the last time anyone saw her on September 5, 2005. She was reported missing by her roommate the next day, September 6, 2005, which was Labor Day. Classes at the university had not even begun yet.

When police started their investigation of what was initially a missing person report under suspicious circumstances, they fairly quickly exhausted their general suspect pool. They interviewed and eliminated people she had come into contact with, including people she had come to the VCU campus from Vienna with – other incoming freshmen that she knew from her hometown.

They eliminated people she had seen at social parties within the week or so when she was on campus. They eliminated people she had come into contact with on her residence hall floor. So they were quickly out of leads.

What is unique about this particular investigation is it is one of the first times law enforcement turned to her online friends, such as her friends within MySpace, to basically expand that suspect pool. Fairly quickly they focus on a guy named Benjamin Fawley, a 38-year old man.

Now, one of the reasons that he caught their attention so quickly was that he was not considered to be "age-appropriate" for her. All of her other friends on her "friends lists" were people who either were in her age group or people who were in her older brother's age group. His name is also Ben and these people were known by him. This Ben Fawley is an outlier.

A little bit about Ben, he is a self styled or self described, anarchist skate board dude, an aspiring fashion photographer, and an aspiring commercial artist. I know a lot of people have lived in college communities from time to time. There are people like Ben in every college town. People who came to attend a university and either never quite got around to graduating or dropped out and liked the atmosphere of the community and just stayed. They have grown up and are still living in their college community.

That was Ben. He was actually a student at VCU. He was in his 12th year of undergraduate studies – studying drama and theater. Initially, law enforcement looked at Ben's online social networking. They found a popular website called Deviant Art (www.deviantart.com) . Despite the name, it is actually a very well respected social networking site where artists of all different genres can post their art and get critiqued by other artists. So if you are sculpting, you could submit a photograph of your sculpture for others to view and comment.

Ben actually posted pictures of Taylor as a model on this site. Some of these photos met the definition of child pornography in the Commonwealth of Virginia. This provided the probable cause that law enforcement needed when they found these photos on this website to get a search warrant for Ben's apartment and his computer.

When they seized his computers and his storage media, by doing the proper computer forensics examination of the box and of his hard drive, they found that he had studied Taylor by reading her Live Journal postings. So he was learning about her by reading what she had written on her blog on Live Journal. When we think about a weblog or blog, think about a diary that you had as a kid or your sibling may have kept as a kid. A diary is where you may have written down your deepest darkest feelings. You lock it away, you put it under your bed and you'd die if anyone ever saw what you wrote in the diary.

That is the same thing people often use blogs for, to record their deepest thoughts and feelings. That is what Taylor did on her Live Journal blog. These can also be useful to law enforcement because bad guys use them too. We have solved cases because we have found blogs of criminals. Bad guys blog and bad guys' relatives blog. So these weblogs can be a double-edged sword.

So law enforcement knew Ben had studied Taylor. So during the forensic examination, it was discovered that while Ben and Taylor were getting to know each other, they found out that Ben had brought Taylor daisies on one occasion. They find out that on her Live Journal blog she talked about how when she was a very young girl, her parents had gotten a puppy. She grew up with this dog, and the dog had died recently. She talked about how sad she was that she had lost this companion of hers.

Law enforcement also discovered that Ben was instant messaging Taylor and chatting with her in social networking forums about his love of dogs, his love of animals, and about how much he loved having dogs around. So it is discovered that as their relationship deepens, Taylor is probably thinking to herself that this guy is perfect for her. He knows her heart and he is just like her. However, what is really going on is he is reading her dairy, her online Live Journal blog, because it is out there for everyone to see.

Now, investigators do not know to this day the true nature of their relationship. Ben says they had engaged in an ongoing romantic sexual relationship. Taylor's friends say that she had a boyfriend of three months to whom she was faithful and monogamous and it was just a friendship. We know that Ben and Taylor at least had a friendship.

We know that on the night of her disappearance, they had agreed to meet for her to borrow a skateboard from Ben because Ben had been teaching her how to skateboard. We know that, incidentally, because the nature of their communication was such that they had left forensic trails on his computer and his computer had been found. That is the benefit for law enforcement. These things can be found if you know where to look and have those resources.

Ultimately, what police found on the Internet during the forensic examination led them to her remains. They did not meet on social networking sites. They met somewhere before. During the second weekend of June, Taylor wanted to go see the VCU campus where she was going to live. Her dad brought her to a friend of her brother's house where they stayed at the VCU campus. This friend was someone who was known to the family. Taylor spent the weekend there. Unbeknownst to her father, Ben was also staying with this family friend of her older brother.

Two weekends later on the first weekend of July, Taylor wanted to go back and see the campus again. Her dad dropped her off a second time at the same friend's residence. The dad did not know that the friend was gone for the weekend so she spent the whole weekend with Ben being at the home. The investigators who have gotten to know her father very well have said that her father said that was the biggest mistake of his life, not going into the residence to check to see who Taylor was staying with that weekend.

So she met Ben in real life. When she came to campus in the fall, their friendship deepened through their communication on social networking sites. All of the information they found led to Ben's conviction and sentenced to 30 years in prison. A large part of the information came from what investigators found on social networking sites.

Ben says they engaged in masochist sex and that Taylor liked to be strangled during sex to increase sexual arousal. He said she accidently died and he got scared and dumped her body so he should have been charged with improper disposal of a corpse which is a misdemeanor in the Commonwealth of Virginia and not with murder.

Because of the state of decomposition of her body, it was difficult for the police to determine the cause of her death but they did determine it was homicide. They could not determine if she was strangled, shot or stabbed. Also because of the state of her body's decomposition when she was found, police could not determine whether she was sexually active with Ben or anyone else prior to her death. So that is one of the reasons for the low sentence.

This is a search warrant that was used when law enforcement searched Ben's apartment, 407 North Hancock. I wanted to show you that address for a second and I want to show you the time. They executed that warrant night on September 28 after she was reported missing on September 6. Her body is found after that.

This search warrant list is very typical of law enforcement finds. You will see in here that you will find multiple loose hard drives that are not hooked up to a personal computer. There are also multiple storage devices – thumb drives, compact disks and digital video disks. One of the things that police took during the search warrant is the digital camera. That ended up being a key piece of evidence in the case. This is why it is so important that law enforcement gets the training because often times digital cameras can be overlooked during a search. The FBI came in and did the forensic "vacuuming" afterwards.

Now I want to show you something real quick, there is no sound to this. This is the last time Taylor is seen alive. This is about a little bit after 10:00 at night and this is taken from a

surveillance camera at her former residence hall. We know that Taylor and Ben had arranged to meet either for a date due to Taylor's blogging to allow her to borrow a skateboard from Ben and you can see Ben right here.

Now while you are watching this, remember, at this time this campus had an open dormitory policy. Ben could walk right up to Taylor's room to meet her without being challenged by anyone if he had chosen to. He didn't choose to do that. Also remember that Ben is 38 years old. Does he look 38 years old to anyone in this room?

You might try to get an idea of what you think he thinks he is doing while he is waiting for Taylor. I have drawn my own conclusion and law enforcement believes they know exactly what Ben is doing while he is waiting for her. I sort of think this part is called the "Vampire" segment because he will never cross the threshold. He walks up to the threshold but never walk in.

Now you see Taylor walking off with Ben to her death. Again, to this day, law enforcement does not know at what point this turned into a consensual encounter or a nonconsensual encounter or what triggered her death. We just do not know. Ben has made his own statements but, obviously, those can not be relied upon.

Now I want to show you the pervasive nature of online social networking sites. This is the van that Taylor got into the night she disappeared. Social networking is such that even the van has its own social networking site. This is Yahoo Geocities, a social networking site, and this van has over 150 representations of it in various states inside and out. If found by law enforcement, this can be helpful to investigators to know the various points of time, and what the van looked like inside and out.

If you look at this particular website, it actually links right to Ben. If you look at this picture right here from that website, you will see "Skulls" right here. "Skulls" is Ben's screen name or user name for most of his social networking. Ben usually goes by "Skulls" or "Skulls_67" or "Skulls_1967" or something similar to that because, of course, Ben was born in 1967.

He uses the moniker "Skulls" because in his artwork and photography he likes skulls. He particularly liked to take photographs of women he meets and superimpose X-rays of skulls over their faces with double-exposure.

Law enforcement found a few photographs in Ben's online Photo Bucket account which is an online social network that has about 48 billion photographs at its site. These are two of them that are on Ben's Photo Bucket page.

Most social networking sites strip off the metadata or information that is taken by a digital camera related to a photograph. This metadata can include things like the camera's serial number, the model of the camera, the date the digital photo was taken, the shutter screen, the aperture, and things like that. Photo Bucket, because it is designed for photographers, leaves that information on the digital photos posted there by site users.

So law enforcement noticed Ben loaded these photos on his Photo Bucket webpage on September 7th, two days after Taylor was last seen. Then when they were able to seize his computer hardware and the digital camera I mentioned earlier, they were able to trace it back to the computer that was used to load these digital photographs on Photo Bucket. So they had a better time on it. Then they found the camera they seized matched the serial number to the camera information on the digital photographs on his Photo Bucket site.

When they matched the date and time clock on that camera up to real world time, they were able to state that the camera took that photo on September 6, 2005 at exactly 6:47:53 that morning. This is exact, beyond a reasonable doubt, objective evidence.

So police wanted to find this location because they knew Taylor was last seen at 10:00 at night in his company, and he is the prime suspect of theirs, and they know he took this photo eight hours later. They took this photograph around and showed it to a lot of Ben's friends and one of his friends says "oh, I remember that location, that is next to the farm house we used to party at a few summers back and I can show you were that is at."

So police went to that location, drove down a dirt road and recovered Taylor's body. Ben's online social networking practices directly led to the recovery of her body. Also his online social networking practices directly tied him to this crime. This is direct objective evidence.

We also know he posted pictures of the dump site. He also posted this photograph of this poem between the time that he killed her and the time he was arrested. They traced this photograph back to a headstone that he took with this camera in a cemetery outside the campus and this photograph of this poem. This was actually on his MySpace page.

The prosecutor blew this up to poster size, put it on an easel and showed it to the jury during opening and closing arguments. After deliberation and after Ben was convicted, one of the jurors said publicly that having seen that poem helped him reach his decision on Ben's culpability more quickly.

Now, this is not an admission or confession, but it helped at least one juror reach conclusion of Ben's state of mind and his culpability in the crime. That's the value of finding this type of information when it is out there online.

This is actually a self portrait of Ben. He posed it himself. That is what he describes as his "bondage bed". Over his right shoulder you see some of his artwork containing skulls. Also noticeable for me is a hyperlink back to one of his Yahoo Geocities pages. I know it is hard to read but I want to show you this particular page so you can see what value it would be to law enforcement if they can find it.

If they can find this page before they interview the suspect in this case, it gives them everything possible they can know about him. If he is in a NASCAR photograph that is shown online, I am going to use that to talk to him in an interview. If something online shows he is religious, I am going to get down on my knees and pray with him. I will use whatever it takes to get an admission or confession, I want to use to build those bridges.

This is what Ben put up about himself. All of this information including all of this stuff here talks about Ben being adopted at birth, the first time he met his mom and where she lives. He lists every city he has ever lived in and where he was born, every state he has ever visited, a separate link to everything about all of his schooling, these are all the places we could ask for a search warrant to if we needed to do so.

It shows all the jobs he has ever held, every place he likes to party and everyone he likes to hang out with. There you can see paragraph after paragraph of what he likes to do, where he goes. He is interested in "goth" culture. This information helps me know what his screen name is at Photo Bucket so I can do searches. It shows the instant messages services he uses and what he buys and sells on eBay. IT talks about when he set up his computer here for the very first time. It talks about how he built his first computer, what it was like and how he has gotten better at building computers.

So what this shows me following an online computer search is what Ben is like and what we need when the computer examiner comes with me during the search. We want to be careful about things like encryption and all of the security countermeasures. All of those kinds of things are available on this particular site.

All of this information is available to me before I even get to the biography page, which has even more information about him. He has put this information about himself voluntarily. It is an open source for law enforcement and just about everyone else to find. What is always embarrassing to law enforcement is when the media finds this information before we do. This is very common, actually, when we find out about it because it is on the 6:00 news.

This part got my attention right here, what he put down when asked about his age: “older than I look, as young as I feel”. With Ben, this is probably pretty accurate. This link right here is to his Photo Bucket page on the Internet.

Now I want to show this to you because when you look down the left hand side of the screen, these are separate albums, each with a bunch of photographs within them. There is one photograph that says “407” on it. Remember 407 North? The address on the search warrant. I will tell you from a law enforcement perspective there is nothing better than when you have photographs of the interior and exterior of the address of where you want to execute a search warrant.

If it is a high risk warrant, my task force team will need this information. If it is a low risk warrant, I at least want to know what the premise looked at points in time so I can coordinate my search. All of this information is online and Ben put it up there waiting for it to be found. His online behavior is not “atypical”.

Let us say my probable cause is a little bit weak and I want to establish more probably cause for a search. Well there is this dope up there for people find. If I want to find people to interview, female after female, he has their pictures. I can see where they were at together and when. This information was just waiting for law enforcement to find. That is the power for law enforcement behind social networking, again, a double-edged sword.

He also has Live Journal pages. What is the value of this? See the skull motif in the background? Let us go into his user information where it shows information about him and all of his friends. If you scroll down here you will see “jail bait” spelled backwards. So he can no longer claim “I did not know her, we were not friends,” because, the way Live Journal works, in order for that user name to be on his page, he has click “Yes, she is my friend”.

So it is no longer a subjective matter. It is objectively his friends because he clicked the button that says they are his friends and they are added to his page. It is no longer up for argument. That is the matter of fact if you can find it. This takes you from the subjective to the objective and basically defeats one of the defenses that someone could potentially use, plus it gives you all of his other friends.

Deviant Art took a big hit publicly because they unknowingly allowed the posting of child pornography. That is one of the few sites that is actually down for them. They pulled it down. The other one is that his MySpace profile is pulled down.

Now, I told you earlier that there were a couple of reasons police focused on Ben. This is the other one, this is some of Ben’s criminal history. Each of these represents separate events and multiple charges for separate events. And more of his criminal history. And more of his criminal history. And more of his criminal history. And more of his criminal history. And more of his criminal history. And finally, a case involving pursuit with a stolen vehicle. These are all property crimes, not violent crimes.

However, there are two protective orders from two females in the proceeding 24 months had filed police complaints for stalking, harassment and intimidation against him. So when Taylor started to befriend him, did Taylor know what she was getting herself into with this guy?

It is not just Ben's profile that is still on line. This is Taylor's profile, still up and live. If you look here, the last time that she logged in, September 4th, 2005, is the day before she disappeared. It is very common for users of MySpace and other social networking sites to use it on a daily or multi-daily basis.

This is a challenge for law enforcement. Publicly, people say law enforcement should have undercover accounts and those sort of things. One of the challenges is that unless you have huge volume of time to devote to it, it is very difficult to keep up that undercover persona.

Now I want to show you this one comment right here at the very top. This is Benjamin, her older brother who is a few years old than her. It says here "Happy 19th, sis. Love you.<3, Benjamin." Now if you think about this, the place that her older brother was most connected with his dead murdered sister is MySpace. If you ever question the significance of online social networking in the lives of people about 25 or 30 years old and younger. Think about that. Of all the ways that he can wish his murdered sister a happy birthday greeting after she dies, he chose MySpace. That's where he goes to feel close to her. That is the significance of this to a lot of young people's lives.

Taylor's Live Journal page is still up also and if we go here to the archives you would see all the diary entries, the same ones that Ben read. And we know he read them through the forensic examination of his computer when he studied her.

Now we move on to a different case, another homicide or another death investigation, I should say. This particular one has not been fully adjudicated yet so I have to discuss that as "alleged."

This one happened on March 11, 2007 and involved Summer Lytle Phelps who was four years old. Her biological mom is out of the picture. It took law enforcement about four months to locate her biological mom to notify her that her daughter was dead. She was living in a household with Jonathan, her biological father who is 28 years old, and Adrianna who is Jonathan's wife of one year, a 32-year old. Jonathan and Adrianna together have a biological baby that is one year old.

Back on March 11, Summer is taken to Spokane Community Hospital and is covered in human bite marks and dead on arrival as a drowning victim. During the investigation that night, police find that she had been engaged to a dog collar routinely as a punitive measure by one or both of the adults. The day her death happened she had soiled her dress and had been made to repeatedly wash it in a bath tub for about a ten hour period.

So police know these circumstances and were going to charge somebody in that household with something but the question is "what can we charge them with that we can prove beyond a reasonable doubt and who, or both, are we going to charge?"

Now, one of the issues of social networking is this. If you go live to Adrianna's webpage you will see a Summer Lytle Phelps memorial page. That is a challenge because of the temporary nature of information, it disappears very quickly. It is irretrievable after a social networking site has been changed or removed. It is irretrievable. You can not get it back. As you can see on this particular site, it was actually updated on March 19. It actually changed on March 17. So you have a six day window to find this and preserve it in a forensically sound manner or you are going to lose anything that has potential of evidentiary value.

Here is what you would have found had you been able to recover this profile in that time period. You would have found all the information about mom, including the interests she would have listed for herself, the music she prefers and three particular blogs. You have a list of her 70 friends and you know what they were saying and who talked to her most recently on her MySpace profile. You even have her sexual IQ.

I will suggest that the information someone puts on their social networking site such as the pictures they load or what they write about themselves is a good indication of their true interests and activities.

So I have the blogs that she has put up and I have a poem that she put up on March 9, two days before Summer's death, where she talks about the fact that it is their one year wedding anniversary. She wrote it in 2002 and tried to copyright it. She is talking about her insecurities of being married to a younger man and how she does not feel attractive enough and her worries about Jonathan leaving her. Now this was as they were starting their new life together.

There is another posting where she writes about how happy she is in her new life and how happy she is to be starting a new family with a new husband and everything is wonderful.

What might be most interesting is the pictures she chooses, these are the pictures. As you look through this, I will explain what most analysts who I have talked to will notice. It is the focal point of these pictures. Summer appears in two of the pictures but she is definitely not the focal point of these pictures.

So, if I am an investigator and I want to assist the prosecutor in developing a theory of the crime, the theory of the crime that I am going to work with is that Summer is essentially excess baggage to Adrianna. She is some other woman's child and an impediment to Adrianna and Jonathan's start of a happy life together. That is essentially the theory that the prosecutor in this case started with.

If I were the prosecutor, I would blow this picture on the right hand side up as big as possible to show the jurors because, in my mind, that tells everything you need to know about what was going on in that household in the time leading up to Summer's death.

So, what has happened since then? The couple separated and law enforcement has moved for two separate trials. They have charged them both with conspiracy to break the spousal privilege**.** They testified against each other as co-conspirators instead of as husband and wife.

They charged them both, in large part because of what they found her MySpace profile, with homicide abuse, which has the most severe penalty attached to it.

The reason I wanted to show you this particular case is because of the value of getting evidence from MySpace to use in trial. Across the country, through no fault of their own, law enforcement is missing this kind of evidence on a daily basis. It is not because of a lack of interest as these are very skilled investigators. It is an issue of lack of training and lack of equipment. In some cases it takes software programs to be able to preserve this information in a forensically sound manner that can beat a defense motion as to whether or not the information is an accurate representation of what was found. Even experienced investigators will miss this type of information.

Here is one more case that I was involved in and it does have some graphic language in it. An Australian undercover officer exchanged photographs and chats with an offender in Indiana. This is a challenge we face in the United States. We can not send child pornography in the process of an investigation. You can ask this, why in the world would I send child pornography if someone is not willing to send it back to me? The answer is one of two things, either they have nothing of value for me or it is a cop I am communicating with. This is discussed openly in these online forums.

However, in Australia, law enforcement is allowed to this. There is a program available in Australia, Google Hello, to do this. One of the things that drew Australia's attention was that in the chats, which were very voluminous, the offender in Indiana bragged about having access to a nine-month old boy and five-year old girl. He sent images that were consistent with him having

access to these children. The Australian undercover authorities then sent the information to the FBI.

Now a little bit of background on Google Hello. This program is a combination of Picasa, which is a photo sharing and file sorting site, and Hello, which is a company that Google purchased that provides instant messaging that allows you to put thumbnails the images right in the chat. This site has become very popular for people who trade child pornography images and other contraband because you can chat about it and have the images up here right next to your chat.

The unique thing about Google Hello is that it creates folders with the full-sized images that you can go back and look at later. Hello automatically puts the thumbnails used in a chat into a folder for the recipient to view later on their hard drive.

You can see here in this slide, this is some of that chat with the Australian undercover. The red redacted lines are the Australian undercover and the light green lines are our guy in Indiana. They are chatting about trading child pornography. This black bar over here represents thumbnail photos of child pornography being sent both ways between Australia and Indiana via international commerce.

Because of the nature of this case, the lead was sent to FBI in Washington and they forwarded the lead to the FBI office in Indianapolis to the cybercrime unit there. I had the mixed fortune of being at a particular United States Attorney's office when this lead came in so I got to work on the case.

Basically, we executed a search warrant, the FBI and the State Police, did at the home of the Indiana offender that night. We did not want to wait any longer because of children being at risk. We used on scene computer forensics and removed the hard drive and we were able to find the evidence on the computer that proved this offender was the right person that we had executed the search warrant on. We were able to find the link to the undercover officer in Australia and recover the photographs that were sent from Indiana to Australia and matched the ones in Australia with the ones found on this person's computer.

Now unbeknownst to users of Google Hello, it creates a file that is not readable by the users but contains information that includes a client user identification, or the user name, and the email address of everyone the user trades with. The offender in Indiana was trading child pornography with over 150 other individual users. Notice, in the part redacted, an @yahoo.com.au email address. That is the Australian undercover.

The offender in Indiana was on parole for five counts of child molestation. He had not met with his parole officer like he was supposed to; he was not working a job that he was supposed to be at; he was not living in the county that he was supposed to be in; he was essentially "off the grid".

This is the sad part of an overall sad story, he was living with his fiancé and they were living in her former mother-in-law's home because a few years previously his fiancé's husband and two kids had died in a car crash. So she moved in with her former mother-in-law to save on expenses and when the offender got out of prison, he moved in with them.

We had time to conduct on scene computer forensics for about 45 minutes because, coincidently, they were out delivering wedding invitations throughout town at the time of the search warrant. He initially denied everything until we confronted him with what we had pulled of his computer. We printed out on a printer what we had found before he returned. At this point he gave us a full admission and actually implicated others.

The nice thing about this is that when you combine social networking with computer forensics, you get some great offender linking. The challenge is though, as you have heard from other

officers, is they are overworked. There is no way I even have the time to send out the other leads to all 150 jurisdictions that were involved in this case.

We were able to have one of the State Police computer forensic examiners go through all those images and the 150 folders and found three that were trading in sadistic images. Among those three there was one with highly sadistic images. In my experience, these were the worst I had ever seen. We put personal attention to that file.

I am now showing you some of the chat that we were able to recover between the offender in Indiana and a new offender who was living in the upper peninsula of Michigan. Over here are the child pornography images and this is how Google Hello works. He sent a picture from Indiana and here is the picture and when there is a picture sent from Michigan to Indiana, the picture is here. Full sized images of the pictures are on both computers located in Indiana and Michigan. Actually because of the social networking aspect, this particular passage came into play where he talks about destroying the camera.

I want to show you the volume of trading going on here too. Seventy images going to Michigan and 70 pictures going back to Indiana. This is very common. We are seeing a lot more volume images going on with social networking with a lot more sadistic components to the images on these kinds of investigations.

We took the log file that was created from Google Hello in this case and typed the yahoo email address that was connected with the Hello account and did a text search. Nothing came back. I took the first part of the email address “poke” followed by four numbers and typed that in and found an eBay account found with a Google search that matched that part of the email address.

I contacted eBay and said “do you have this account?” They said yes and they would email the information to me after I sent them a subpoena. I sent the subpoena with the email provided and eBay sent me everything about this guy. Bank accounts, PayPal transactions (PayPal is owned by eBay), name, address, phone number, purchase history, credit card information was sent to use from eBay. This also included this disturbing purchase history. Remember the camera that he broke? This is the digital camera he purchased from eBay. It was old enough that the information had aged in eBay’s system but it was still cached in Google so that we could recover it online.

When you have trained officers, they can go and uncover things like that. Here is more of his purchase history. There is the camera he purchased. He bought extra memory for it and he bought a tripod. As we started looking through his purchase history we became concerned. We knew from our investigation that he had part time custody of his nine-year old daughter.

He shared custody with his divorced wife. This was not something a 41-year old adult male would be likely to purchase. More likely, it would be bought for a child. Remember the timing on this. One camera had been broken, and a few months later he was buying a new camera for himself.

The camera comes into play, because, about two days into the investigation, coincidentally, the 15-year old female babysitter who watched the 9-year old daughter walks into the Michigan State Police post with a DVD and a VHS tape. She says she found these pictures. He has been taking pictures of me in the bathtub.

This is a rural area. He is a licensed practical nurse. He works overnight at a nursing home. The 15-year old would spend the night at his house watching the 9-year old daughter in case she wakes up scared in the middle of the night. In the morning, the babysitter would take a bath the offenders home before going to school so she does not have to return to her home on the Indian reservation in the upper peninsula of Michigan.

The babysitter finds a hidden camera and, when he goes to work, searches his bedroom drawer. She finds tapes, watches them, and finds compilation tapes and DVDs of her in the bathtub. She

brings them to the Michigan State Police. They obtain a search warrant. Among the things they find are a 12 megapixel digital video camera. This brings us full circle. They also seize a laptop computer. As I testified at the federal detention hearing, the laptop contained over 400,000 child porn images. Among them, over 3,000 were sadistic in nature. Over 500 depicted genital mutilation of children. Included was the only video I have seen that depicted genital mutilation of children. I had never seen that before in my limited experience.

The federal magistrate, a retired FBI agent, asked me to define the difference between sadistic images and those of genital mutilation of children. I explained to him that causes permanent scarification or damage to the child. He detained the individual, and as only this particular magistrate could, explained to the subject that he hoped he never, ever gets out. If he could, he would do worse at the detention hearing. There was no bond. The subject was detained.

That is the value of computer forensics. We did this in the southern district of Indiana because the western district of Michigan did not have enough to charge him until the forensics were completed. We had enough to charge him in Indiana because of the receipts, but could not charge the distribution.

How did this work out? Our guy from Baseville, Gerry, was sentenced to 200 months.

I would like now to talk about the development of our mobile forensics lab and its deployment. Being able to do mobile forensics on scene makes a huge difference in investigations. This relates to the time value of evidence. When equipment goes to a regional laboratory, even if it comes back a month later, the value of the results, and incorporating those results with the service provider records and IP logs is gone. That type of information can not be recovered.

The individual in Michigan, Kenneth Wayne Miller, was sentenced to 33 years and will serve 80% of that.

This shows the nature of on-line social network. It is a double edged sword. The path goes from Australia to Indiana. The Indiana subject, Gerry Browder, gets 292 months. The subject in Michigan gets 400 months, followed by lifetime supervised release. The sentencing district court judge prohibited him from ever coming within a 100 yards of a child for the rest of his life. If he does, he has to notify his probation officer immediately and the child's parent or guardian. This may not matter since he will be 74 when he gets out.

We sent a lead out to Delaware dealing with some sadistic images. The wife of the suspect turned out to be on the school board. The suspect himself is the girl's lacrosse coach. He was detained and died awaiting trial.

The third individual went to Georgia. He was searched. A complaint was issued. He is still pending trial.

But remember, there also were 147 we could do nothing with.

To illustrate how these items build up, Dirty Hello is a stand-alone web site for people who want to use the Hello social networking application to do bad things – to talk about things of a sexual or violent nature.

But, don't worry. For what ever reason, and I will not draw a conclusion, Google decided to pull Hello. So Hello is no longer available. This would solve the problem, except for the fact that the FBI has located three new sites to cover the gap. Some seven weeks ago, Google launched a new application called Lively.

Lively has all the features of Google Hello, but now adds a visual dimension. This is a virtual world where you create an avatar to look like you want. You can create a room where you can

hang out visually with other avatars. And, your avatars can trade files back and forth and chat. I do not want to pick on Google here. There are also a number of other sites. IMVU is another. It stands for “Instant Messaging Virtual Universe.” IMVU has its own economy with virtual money that can be traded for US dollars.

If you think of the psychology of someone who trades in child pornography, you can think of how attractive it must be to create an avatar with whatever appearance you want and be able to trade with people who help you to justify your lifestyle.

[BREAK for 5 minutes.]

AG CORTEZ MASTO:
Are we ready to get started again?

SHERIFF GILLESPIE:
Madame Chair, I am going to have to excuse myself at 11:45. I have a noon appointment.

AG CORTEZ MASTO:
We will probably go about another half hour. We are going to talk a little about Second Life, and then want to open the session for questions. Lt. Cohen, are you ready?

LT COHEN:
I am, thank you.

The Legislative Staff IT personnel have asked that I repeat my disclaimer. You may hear bad words, not all that bad. You may see naked cartoon characters. Because we are cutting back a bit, I will skip a few slides as we go on.

I want to talk about massive multi-player on-line games and multi-user environments, or virtual worlds. This demonstrates changes over time. If you look at 2008, we are at 14 million users of massive multi-player on-line games like World of Warcraft and RuneScape. This is a projection of growth over time. This will be a big problem for law enforcement across the world, including the US.

A lot of games have hit and show an increase, particularly this year. Habbo Hotel has 90 million registered users. Many people have not even heard of it. IMVU, which I just showed you, is right up there with 20 million registered users.

I am going to talk about Second Life as an example because it is probably most well known, but it only has 13 to 14 million people as registered users, depending on how you do the math. Despite the fact that it is US-based, and we will be talking about it, it is not as big as some other virtual world sites.

Some of you will have seen references to Second Life in the media. Let me explain a bit about it, before going into criminal uses so you have an idea of how it operates. It is not a game. It is a multi-user virtual environment. It is owned by a company called Linden Lab, based in California, but with international service.

You use your avatar to go to a virtual job to do your virtual work. You go to the virtual water cooler to talk to your virtual coworkers. Afterwards, you go to a virtual bar and have a virtual martini, which you pay for using real money. I will explain the money aspect in a moment. Then you might go to a virtual after hours club and have virtual sex with another virtual avatar. You might make a movie of that called “mashinima” [or “mashinama”] because a movie filmed in virtual life is called “mashinima”. You may sell that for more Linden dollars, the currency of exchange in Second Life, to someone who is interested in buying mashinima of people engaged in sexual activity. That is essentially how Second Life works.

I spend about three hours last night and over an hour this morning talking with a law enforcement entity on the East Coast about an on-going case. They just had an 11-year old girl, who was tortured and murdered. The primary suspect spends 20 to 23 hours a day in Second Life and other virtual worlds. He has no real life friends. Their learning curve started with the question, "What is Second Life?" These are people in the Internet Crimes Against Children (ICAC) and cyber crimes task force.

Their suspect is involved in the fringe, extreme element of what occurs in virtual worlds. They believe that the girl was somehow connected. This demonstrates the relevance of this information. We are not dealing with hypothetical crimes that are being committed.

This is different from a game. You do not have winners and losers. You do not have a score. You do not have goals. You are not trying to get to the next competitive level as in World of Warcraft, RuneScape, or John Madden Football Online. You do not play, you simply be.

I want to show a video very quickly. This is the quintessential video that explains second life. It was crated in 2005, so it is a little old.

VIDEO VOICE INTRODUCING SECOND LIFE:

This video is mashinima, video film in Second Life, about the world. I am going to explain to you about Second Life and many of the companies that are using it to their advantage.

Second life is an immersive 3-D virtual world. Users control their avatars to create content in their on-world experience. They make their own list of friends and can join or create groups. They communicate with other avatars by chat or instant messaging.

Users in Second Live own the IP [intellectual property] of whatever they build. They can also buy and sell objects with real money. Second Life has its own currency of Linden dollars and a foreign exchange called Lindex – the Linden dollars created as US dollars.

There is already a social networking system in place. They can meet in Second Life friends from the real world and have discussions, debates, and transactions. Innovative businesses are starting to explore the potentials of these new worlds. Durand Durand is setting up band community island to be opened in the near future. Warner Brothers is promoting a movie special in an New York style loft.

As you walk through that loft and click on objects, it takes you right through the Second Life loft to an old fashioned web site.

Star Wars fans have built a Star Wars set in the sky. They can have regular role plays and also enact scenes of their own imagining.

In the future, the graphics will be realistic, and so mashinima could have a significant effect on the film industry. Zero cost, highly professional production facilities also encourage creative talent around the world and in all walks of life and age groups.

Canadian mobile carrier Telus and Adidas have stores where one can buy mobile or a pair of shoes for one's avatar. Mobiles are totally useless in Second Life, but all the more for having one. Retailing in Second Life includes product placement, advertising, store layout design, and product testing.

Second life could be used for market research, trend spotting, and feedback. In the future, consumers can collaborate with firms to design products in Second Life. Outsourcing could also be a way for solving problems by cooperation. Real life dress on the left, virtual one on the right.

Games could be designed and created in Second Life. A game developed and tested in Second Life was then licensed to a real live company. Looking at this game in progress shows how complicated multi-dimensional and fast trending information can be displayed and acted upon quickly in a virtual world, much more powerful than traditional computer interfaces. Perhaps stock exchange information could be displayed in 3-D visuals for quicker and easier absorption.

Second Life has professional architects, artists, and designers using Second Life to easily model, display, and sell their work. A Stanford student has used it to implement mathematical concepts such as a Klein bottle. It creates an interface for self expression. Starwood Hotels is building a new hotel in Second Life that will not open until 2008 to collect feedback influencing the eventual real life hotel.

Universities such as Harvard already hold live debates and panel discussions in their virtual campuses, which are simultaneously broadcasted by a traditional radio. Here is an example of classes on complicated topics being taught in a virtual classroom. Both teachers and students are interacting through their avatars. It is likely that languages will soon be taught because Second Life enables one to practice in an engaging setting. One can also meet people native in the language in one's real life or communicate with multi-lingual robots and objects.

LT COHEN:
What you have seen is what Second Life is. An avatar is the character you are creating. Furries are non-human avatars. These constitute an entirely different race. Another Second Life term is "griefing". Griefing is anything that annoys another avatar or anything that is criminal. Be prepared for your desk sergeants to have someone come in and complain that they have been griefed – "Someone stole 500 Linden dollars from me. I want to report it."

They want to report a real crime. In Indiana, we put people on front desks because they cannot interact with people in the first place. Now we have someone who wants to talk about being griefed in a virtual world. This will not go over well. But the victims are real people who are victims of real crimes. They want to report the crimes that have occurred in a virtual world. This is big business. It is of enough concern to law enforcement and intelligence communities that I just returned from a month in California attending a think tank session sponsored by the Director of National Intelligence. They need to do a national intelligence assessment on these issues.

The CIA is now doing most of its non-classified meetings and briefings in Second Life simply so their analysts can become familiar with the platform. The CIA sees a need for that. The analysts need to be familiar with what is going on.

This is what Second Life looks like from the air. This is a snapshot of islands. Some of the islands are BMW, Toyota, Pontiac, and Mercedes. You can enter the island and buy a virtual car or you can buy a real car. Your purchase can be in Second Life using Linden dollars as a currency of exchange or you can use a real credit card.

Earlier this morning, you heard other investigators explain various issues. Now there is a second platform, a virtual world, for doing exactly what has been reported.

Five countries now consider Second Life to be a sovereign nation. Sweden is the largest country. Then there is Estonia and three countries in Africa no one really cares about. This is the Swedish Second Life Embassy. You can do everything in the Swedish Second Life Embassy you can do at any other Swedish Embassy anywhere in the world. Architecturally, it is modeled after the Swedish Embassy in Washington DC. You can apply to replace a lost passport if you are a Swedish citizen. You can apply for travel documents. You can actually apply for asylum if you want to.

The United States does not consider Second Life a sovereign nation. Second Life does not have a seat at the UN, but you can see where the trend is going.

Looking at the Swedish Second Life Embassy from the air, think of these borders as the compound walls. When you own an island, as Sweden does, and as businesses do, your island has your laws and your rules. It can be an open island where anyone can land on the beach and do their business. It can be a semi-closed island where a fee is paid, or a password is used, to get access. Or it can be a completely closed island, like the ones the intelligence community uses so that no one can enter except if they are identified from a pre-approved list.

If I want to enter the Swedish Embassy, I land here, and am challenged by the embassy guards. They are real people controlling avatars in real time in order to talk to me. There might be a receptionist, who is a real person, a real Swedish government employee who is doing something. There is a genuine Swedish government job identified as the Ambassador to Second Life. Since we have decision makers in the room, let me identify my life goal: to become the first US ambassador to Second Life. If you know someone, please pass that on.

Two semesters ago, Harvard had nine courses available through Second Life. Last semester they had 15. I do not know how many will be hosted this semester, but they have a stated goal that by 2015, a Harvard Law Degree will be offered that can be obtained solely in Second Life. Harvard is just one of many schools that are setting up platforms as islands in Second Life. John Hopkins Medical School has an island where they simulate schizophrenia for research. Lots of businesses are doing work both retail, customer outreach and marketing. They also hold internal meetings.

One sector that lags behind is public sector law enforcement as well as the intelligence community. We are behind in our use and understanding of this environment.

Users of Second Life are not just a few guys who live in mom's basement. In February of last year, there were 30,000 concurrent residents. Now, 24 hours per day, 365 days a year, it is rare for the concurrent population to drop below 65,000. As of this week, the number of total residents is approaching 15 million residents. Of these, half a million logged on in the last seven days.

Second Life is a large city. Just like any large city, there are criminals in this community.

Last month 30 million hours were spent in Second Life. These are real hours that real people are online. If I do not control my avatar, if I go have dinner, for example, my avatar falls off world. These 30 million hours are hours people are spending in Second Life instead of doing something else. For some, this is becoming their first life. Usage hours indicate that US citizens, whether they know it or not, are interacting with people in all these different countries. There are some islands that automatically translate from one language to another, so there is not the same language barrier that exists in real life.

I will not go into costs in detail, but there are a lot of people that pay a lot of money for Second Life. Last month almost 2,000 new islands were created. These did not exist before. This universe is expanding. Every month there are between 2,000 and 4,000 new islands that are being purchased for a minimum of $1,000.00 apiece.

Linden Lab has just over 5 billion Linden dollars on account. This translates to a real world market value of about $30 million in US dollars. This money is held in trust for people. Linden Lab is not a regulated financial institution. It does not have to comply with bank secrecy acts of anti-money laundering acts. "Know your customer" and banking regulations do not apply.

Linden Lab is US based. I know about this because Linden Lab decided to self-publish this information. Many other virtual worlds, spread out all over the globe, do not self-publish information, but nevertheless, have real world equivalent currencies. What happens of these organizations go bankrupt?

Last July, there were over 200 that made a net profit of over $5,000 that month. This equates to over $60,000 per year in US dollars. Income taxes on these funds are being paid completely on the honor system. No one is receiving a W-2 of 1099 form from Linden Lab because that is not the relationship a participating company has with Linden Lab. The transactions mostly go through PayPal, and now, some additional sites. PayPal's accounts are not interest bearing, so it does not issue any user an 1099 INT. As a result, any US income taxes on real US income are paid solely on the honor system.

Linden dollars are indicated by the prefix "L". The current exchange rate is roughly 2.65 to 1 against the US dollar. The exchange rate fluctuates on the Lindex. Currency exchanges are effectuated through PayPal for a cost of one dollar per transaction. It does not matter whether I exchange 1 US dollar or 10, 000 US dollars, I still pay one dollar in each direction for that transaction.

Formerly, only PayPal could be used. Now, Linden Lab offers exchange facilities to a number of other exchange companies. Most of them are not US-based. As a result, law enforcement can not reach them through legal process. Perhaps this can be done through federal contacts using the Mutual Legal Assistance Treaty or through a local FBI legat (legal attaché). There are lots of "maybes" in this process. You can see here how the exchange rate varies somewhat against the Euro depending on which currency exchange is used.

It is very easy to transfer money in and out of Second Life. It is so easy that Reuters, the international news agency, offers a free currency converter throughout the day so I can see how my Second Life money is doing against the US dollar or some other real world currency.

Last July, there were 593 enrolled residents who spent over a million Linden dollars. There were 296 individual transactions that were over half a million Linden dollars.

The Linden exchange shows both an opening and closing rate, so I can make or lose money simply by playing the money market in Second Life – exactly as I could by trading in the past German Deutschmarks against the US dollar. However, in the real world, currencies fluctuate based on real world considerations. What are Linden dollar fluctuations based on? I do not have the answer to that. Lots of money is being exchanged.

Now, let's look at some of the potential for financial crime. There is potential for insider trading. There are no regulations in place. Technology has advanced before current statutes and legislation.

From my experience, Linden Lab is very helpful to law enforcement. They run a good site. They are making so much money legitimately; they do not want criminals on the site. I can not say that about other sites.

Can you imagine being a financial crimes investigator and having to do a profit and loss statement to prove that this is a fraudulent business operation with virtual profits and losses that operates in multiple virtual currencies?

Theft of intellectual property is a huge issue. Last year, South Korea had 10,000 arrests for virtual goods and services. Compare that with the US, where we maybe had a handful. These cases dealt with someone stealing a virtual bed or someone stealing a virtual flaming green sword. That is a real crime because the sword has a real value. Our laws have not kept up with this development.

VOICE OF VIDEO REPORTER:
A strange bit of legal history today in the online virtual universe of Second Life. One avatar that is a cartoon-like online identity that people create for themselves, has sued another for stealing his

intellectual property – the design for a virtual bed. But where do you turn for justice in a virtual world. Ben King investigates. We should warn you. This report does contain some partial nudity.

The oldest profession in real life is also the biggest business in Second Life. While big name companies see it as a marketing opportunity, for many residents, it is a perfect playground for their sexual fantasies. By some estimates, sex accounts for 30% of the Second Life economy. And shops do a roaring trade selling sex toys, lingerie, and artificial genitalia. Avatars, born with no genitals of their own, have to buy whatever they need. That means plenty of eager customers for sex shops like Strokers Toys, which makes hundreds of thousands of dollars a year. Success, which has led it to the courtroom. This is one of its most successful products – the sexgen bed, essential kit for any amorous avatar. Stroker Serpentine, real world name Kevin Alderman, claims that another avatar has stolen his bed design and is selling counterfeit copies. Using a loophole in the Second Life law, the alleged thief, Molkob Katino, and others like him, have been able to escape justice.

They will keep the product they have…

LT COHEN:
The report goes on from there. This should give you and idea of what is going on. For anyone concerned about this being webcast over the Internet, that news clip was played from CNN, so I think we are OK.

Social engineering in credit card crimes – trying to get someone to give me their information so I can commit identity deception – now is happening in a virtual environment. I am using a virtual business to get a real credit card number.

Turning to prostitution, I am now displaying one of my avatars. That avatar was offered sex with a virtual prostitute. She was going to go off somewhere with me.

How about real world prostitution? Turning from Second Life to World of Warcraft, a real case involves a user of World of Warcraft wanted a flying mount. This is a flying character that would enable her character to move around more. She prostituted herself on Craig's List, an online social networking site, where people offer to buy and sell things. She offered herself in exchange for 5,000 gold, the currency exchanged in World of Warcraft. This is equivalent to about $125.00. She found a taker. According to her own Second Life posting, she consummated the deal, and we know see her avatar on her flying mount.

Last month, Kimberly Journagan, 33, in North Carolina, kidnapped a man from Delaware. He is 52. She had formed a virtual relationship.

VOICE OF VIDEO REPORTER:
A virtual relationship turns into a real life nightmare for one Delaware man. Police say Kimberly Jounagan, a postal worker from North Carolina, met Claymont man through the online game Second Life. He later ended their relationship, but police say Journagan wanted him back. She allegedly broke into his apartment armed with a taser, a BB-gun, and duct tape. She waited for him to come home.

She indicated that she wasn't ready to end the relationship and that, if need be, she was going to take him out of the house by force. The man took off and called police, who found Journagan's (sic) dog bound with duct tape in his bathtub and a pair of handcuffs and duct tape outside his bedroom window. Journagan now faces charges of attempted kidnapping, burglary, and aggravated assault.

LT COHEN:
The report goes on. By the way, the dog is OK.

If you are an online pharmacy selling illegal drugs, what better way to market than having a virtual drug? Seclamine is not found in the PDR, the drug bible, because it is a virtual drug. It gets your avatar virtually high. This is a marketing technique used by people who want to sell real drugs.

Now, how do I do a lawful communications intercept when someone is using Second Voice or instant messaging? There are ties to user groups, and I will show you some examples.

Another topic is online gambling. Thanks to an operation by the FBI and IRS, this has been cut down on Second Life. It is diminished, but it still exists. They just go about it differently. If one online community stomps down on it, it doesn't go away, it moves somewhere else. So, now, a number of other virtual universes have sprung up to fulfill the need for virtual gambling.

And, now, money laundering. This is how money laundering works. If I want to launder money in Second Life, I take $10,000 dollars and purchase and on-line Picasso. There are two ways I investigate money laundering. I can do it by cost of goods sold, or by fair market value. I create an alternate avatar and a virtual account for the alternate avatar. I take that $10,000 and change it to 265,000 Linden dollars. I then buy that virtual Picasso for 265,000 Linden dollars, and then cash it back out for $9,998 dollars. I have now effectively laundered $10,000 for a two dollar fee – one dollar to PayPal in and one dollar to PayPal out.

There are two ways I can prove money laundering, fair market value and costs of goods sold. What is the cost of goods sold if the good is a virtual Picasso? Second Life is a program, the transaction is all ones and zeros. There is no cost of goods sold I can prove. What is the fair market value? I can tell you, and I can prove beyond a reasonable doubt what the fair market value is of a real Picasso. What is the fair market value of a virtual Picasso that has never existed before. No one has ever wanted one before. No one has ever bought or sold one before. Apparently 265,000 Linden dollars. That value has now been set, so I can replicate that money laundering transaction over and over again.

And we have not talked about the steps possible to conceal the transaction. This is an out in the open transaction, simply one that law enforcement can not prove.

Second Life does try to catch these schemes. A number of businesses have sprung up, so you can actually do this off the Lindex.

This blacked out side, offers, for eleven cents on the dollar, a way to bypass the Second Life controls whereby Second Life tries to monitor people doing the transactions I just described. Actually, this particular eBay page links to a web site for the company that offers the opportunity to complete the transaction in a number of virtual currencies – all for between 10 and 12 cents on the dollar as a fee to that particular company. I can transfer funds between US dollars, Euros, and Brazilian real. I can use PayPal, money orders, Visa, or MasterCard.

If you use a number of sources to track back the company location, you learn the company is run out of a non-descript residence on the bay in Miami, Florida. I can tell you that no law enforcement agency, federal or state, is looking at this at all. This individual is one of many others that offer monetary exchanges on line for all these different currencies.

Let's talk about terrorism for just a minute. This is basically how I would conduct an operation in the United States if I were a terrorist and communicate in a manner that is unmonitored.

This is a hypothetical instant messaging conversation between a controller and a cell in an online game called Quest.

MR. EARL:
Those of us in the north are having a hard time seeing what is going on.

LT COHEN:
Let me explain. Basically this is a chat about what is going on during a quest in a virtual online game. It using the vernacular and slang common to a virtual world. If you think of World of Warcraft, at any given time there are 10 million users “in world” from all across the world playing on a number of servers.

If you notice these numbers at the bottom, 124 gold and 235 silver inside, and the other player responds, “Got it.” This is a map from a virtual world and it tells you where to start. If you take that map and go to where one of the players told you where to start – the stone keep. That is another location on this particular map.

If you do not recognize this map, it is an areal map from the Rand McNally Atlas of Washington DC. If you go to the grid on the atlas, and look for that number sequence, you then overlap that on top of the game map and you find the White House.

This is how you can convey an attack order in a virtual world in a manner that is essentially untraceable and unproveable.

How about propaganda and recruiting?

This is mashinima, a movie filmed in Second Life. You can play the characters in one of these islands. This is done on a combat island. You can choose to be one of the Americans, the Iraqi translator, or the Jihadiis. They make a movie of people playing this game. This is an island that exists in Second Life. These are real characters controlled by real people. It continues. It links to a YouTube site and a particular propaganda site, where you can find more movies, including one I choose not to put up here, about how to manufacture and deliver a truck bomb.

AG CORTEZ MASTO:
Lt. Cohen, could you give us just five more minutes? I would like to ensure we have time for questions and answers.

LT COHEN:
Let me turn to age play. This involves islands set up for people who like to dress up like little children and have sex with each other. Emily Semaphore made a million US dollars by operating age-play island. Second Life has cracked down on age play, but it still exists. Instead of having islands to go to, now you go to “playgrounds” and wait for a child to approach you. This is a child avatar controlled by an adult in most cases. Rough play also exists.

The latest booming large business is now made to order, snuff mashinima. Customers will order up a particular scene in which one of the characters gets killed. Someone will create the environment and create the mashinima and sell the movie that is made to order.

Let me leave you with this. This is Red Light Center, another virtual universe. I want to show it to you because, if you notice, the corporate address is a post office box here in Nevada. It is created by a company called Otherverse. Let me show you a very brief video.

VIDEO VOICES:
Hi. I am Red Light Center.

And, I am MySpace.

I am a cool space you can go to make new friends.

So am I. At MySpace you can have thousands of people claiming to be your friends.

Wow. Do you really have time to connect with that many people?

Well, I don't really connect with them. But they are on my list.

The friends on my list have really become my friends. We hang out, go dancing.

Over here, you can even post your picture and leave comments for users for a good time.

Where can't you do that? Oh, here comes one of my new friends.

Um. Ah. Um. Does she have a friend? Hello. Hello?

Hello. I am an avatar in Red Light Center, and I just found a new way to get high.

High? Do you mean like with pot?

Well, actually, it is virtual pot. It gets my avatar really binked.

I could never do anything illegal.

Well, neither would I. But getting virtually high is totally legal and the pot is free.

It does sound tempting. But I spend so much time alone with my computer.

Who said anything about being alone?

Well, maybe just one hit, but I may not inhale.

LT COHEN:
One thing about this particular site makes it different from Second Life. It links up to the Otherverse, which is their traditional Web 2.0 social networking site for people who want to meet for various encounters. This allows you, should you choose to, to go onto the site, and engage in activity in a virtual world. If you like that activity, you right-click on the other person's avatar. That takes you to the Otherverse profile, so you can arrange to meet in real life. It also allows you to choose only avatars that, in the real world, correspond to people within driving distance for you, or where you want them to be. So, you can experiment in a virtual sense, with the intent of meeting in the real world. They have a sister sight that launched in September called VirtualVancouver, which is for people who want to do the same thing, targeted to the drug crowd. Instead of meeting for a sexual transaction, you meet for a drug transaction.

One of the things I want to leave you with, since someone asked about it, is the mobile forensics vehicle our department has bought. We found that the on-line social networking and computer forensics is so closely linked that we do not have time to send equipment to a remote laboratory. We need forensic results right away in order to interview people. We need it right away in order to develop secondary and tertiary evidence. We converted an RV into a mobile forensics vehicle. We do exams in the back. We have had up to three examiners working simultaneously in a temperature controlled environment. The front section has been turned into an interview room that has audio and video, and means to allow covert communications between the front and the back. We can interview a suspect, whether a consensual encounter or a search warrant situation, and at the same time, be doing computer forensics to try to develop whatever forensic compute evidence we have. That is how we have gone about doing this.

Thank you for your time. I will try and answer your questions as best I can.

AG CORTEZ MASTO:
Thank you very much. Are there any comments or questions from Board members?

I think you have overwhelmed all of us.

Let me ask you this. I noticed in your literature a little bit about on-site triage and the need for that in order to relieve some of the burdens placed on computer forensic examiners. Could you explain a little about that?

LT COHEN:
I skipped over that for the sake of time. We have looked at the fact that we simply can not afford to have enough fully trained forensic examiners. We only have four for the entire state in our department. Other departments do have additional ones. We do not have enough to send them to every scene. They provide, essentially, the top part of the pyramid, composed of our cyber-crime forensic examiners. We figure we spend in excess of $150,000 in training and equipment per examiner. Below that we have first responders who are trained so that they can go on scene and do a percentage of what an examiner would do to recover the evidence in a forensically sound manner, in a way that will stand up in court and be supported by the cyber-crimes unit either in real time, or later, when it comes time to testify. Below that, we have what we expect our crime scene investigators to be able to do. These are the folks who do everything from collecting DNA to footprint impressions.

One of the things we do for all of our officers because of online social networking, we have done a two-hour training session for every one of the 1300 troopers we have. The training includes collecting evidence in cases involving online social networks. Unfortunately for me, that ended up as a DVD of me talking, so I am now infamous. We established specific skill sets we expect people in each of these groups to have. We know what roles we expect them to have and what training and equipment we expect them to have. We are comparing $150,000 for a forensic examiner, actually more than that, to roughly $15,000 for one of our first responders. Obviously this is a big cost difference. The program is also a force multiplier.

AG CORTEZ MASTO:
You said this was atypical. So, with respect to the users now, the numbers of individuals that are on the Internet involved in these social networking sites, and particular the younger generation that puts all of their information online in one form or another – pictures, and journals – is that typical now of what we can expect?

LT COHEN:
It is. When I train, I try to explain to people, “Don’t think about a cyber crime unit or cyber crime investigations. You have to think about the cyber crime component of all investigations.” There will be evidence in the Internet cloud and on computers in every homicide, in every burglary. It is going to be there. It may be a suspect researching how to do something in a homicide or sex offense. Or it may be a burglar who is trying to sell swag on Craig’s List or eBay or some other site. The evidence will be there. A suspect involved in a string of arsons may be using MapQuest or using one of the other mapping programs to determine where he is going.

It is hard to find an investigation where there is not something of evidentiary value that relates to cyber crime. Even in a drunk driving case, there is information that can be taken from a users cell phone of evidentiary value. This may be information relating to GPS determined locations coming from vehicles that are equipped with GPS. This is of evidentiary value.

The problem is that we do not have the training, personnel, and time to recover the evidence in all cases.

SHERIFF HALEY:
Madam Chair, I would like to ask, briefly, for a discussion on the litigation side. Once a case gets to court, how well versed are your prosecutors in order to move these cases forward?

LT COHEN:
That is a challenge for us. We have been lucky in that a particular AUSA (Assistant US Attorney) from the Southern District of Indiana, a federal prosecutor, is very supportive of this triage, the staged, tiered approach to investigation of cyber crimes. In Indiana, we have 90 elected prosecutors that cover 92 counties. All of them have various backgrounds in prosecutions and in technology. The training component for the prosecutorial side and the judiciary is a challenge for us as well.

I will tell you though, we have never, not once, had evidence recovered from a first responder that was suppressed, or failed to have it admitted in court. We have been fortunate in that regard. Training is not just about how to turn the computer on, we are providing first responders hardware write blockers. We are maintaining the forensic integrity of the original evidence, so that an examiner can replicate it or build upon what is being done by the first responder. We are trying to do very good documentation of what we did. We are finding that so long as we document what we did, we are not having a problem with it in court. Does that answer your question?

SHERIFF HALEY:
Yes it does. Thank you very much.

MR. EARL:
Could you talk very briefly about the training program to get your first responders trained? I understand there is a link you have with Purdue University. Is that correct?

LT COHEN:
That is another key component. We formed a partnership with Purdue University computer information technology department, National White Collar Crime Center, and our agency. Purdue put together a three-day school for first responders. That is our first step. It teaches them how to use a hardware write blocker, how to recover information, and how to do it in a forensically sound manner. We bring in information from the US Attorney's Office and the National White Collar Crime Center about how to do this lawfully and how to present it in court when the time comes.

So, basically, our first responders first training certificate comes from Purdue University. Purdue stands behind this and its training in how to use equipment and develop skills. We build on that base from there. From Tuesday, for example, our first responders will be going to the FBI's image scan school. While they are doing investigations already, this is just one more tool, provided by the FBI, to have in the toolbox. We are hosting the session and the FBI is providing the training.

I expect a first responder to have the training and capabilities to do roughly 30% of what a computer forensic examiner can do. They are never going to break encryption. They are never going to do a lot of things with deleted or obfuscated information. But what they do, they will do in a manner that does not alter the basic information, and is done in a forensically sound manner.

MR. EARL:
One of the things that has cropped up recently on NW3C's list of training courses for law enforcement is a new course in computer forensic triage. Were you connected with that? Do you know anything about it? How closely that might mirror some of the training that takes place in your training or the Purdue program?

LT. COHEN:
Actually, it is a little bit different. I think you might be talking about their STOP or Secure Techniques for Onsite Preview course.

MR. EARL:
No, they have a more recent course they are calling computer forensic triage.

LT. COHEN:
They were talking about doing one with a hardware write blocker, but it would require some other courses before it. There is an individual who has half of his salary paid by Purdue and half by the National White Collar Crime Center that sits at Purdue University. He has been involved with it. It is a little different from Purdue's course, but it is complementary. They are teaching some live acquisition for the computer people as well as some dead-state acquisition through use of a write blocker. The traditional STOP course does all its training through the software Novix tool.

AG CORTEZ MASTO:
Lt. Cohen, thank you very much for flying out here. This has been a very informative presentation. We greatly appreciate your taking the time. It was an eye-opening presentation for me.

Agenda Item 6 – Board Comments. (Discussion/Non-Action Item)

AG CORTEZ MASTO:
Moving on to agenda item number 6, it is time for comments from Board members. Do members have comments. Hearing none, we can move on.

Agenda Item 7 – Public Comments. (Non-Action Item)

AG CORTEZ MASTO:
Are there any members of the public in Carson City who would like to address the Board? Seeing none, are there any members of the public in the south who would like to address the Board? Hearing none, we can move on.

Agenda Item 8 – Scheduling future meetings - 4th quarter of 2008, 1st quarter of 2009 during Legislative session. (Discussion/Action Item)

AG CORTEZ MASTO:
It is my understanding that Legislative facilities are going to be unavailable from November 1 through the end of session. We have to figure out where we will be located for our next quarterly meeting, is that correct, Mr. Earl.

MR. EARL:
Yes, unless the meeting is held before the 1st of November. I have made several calls to those members who are most difficult to schedule. As of several days ago, October 24 and October 30 are days we might meet within the Legislative facility. If those dates are not convenient, we would have to consider where to meet during November or December.

AG CORTEZ MASTO:
Does anyone have concerns about meeting in October, either the 24th or 30th?

MR. UFFELMAN:
I can not meet on either October 24th or 30th. I will be out of the country.

AG CORTEZ MASTO:
Why don't I ask Mr. Earl to check with everyone about those dates by email or telephone? If they do not work, then we will coordinate the following month and determine where we might meet. We will then get back with Board members. Does that work for everyone? Good.

Agenda Item 9 – Adjournment.

AG CORTEZ MASTO:
Moving on to Agenda Item 9, is there a motion for adjournment?

Motion to was made by Sheriff Haley and seconded by Mr. Ipsen.

Motion to approve adjournment passed unanimously.

Meeting adjourned at 12:25:40 PM.

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on October 30, 2008.

Minutes of the
Nevada Technological Crime Advisory Board

October 30, 2008

The Nevada Technological Crime Advisory Board was called to order at 10:00 a.m. on Thursday, October 30, 2008. Attorney General Catherine Cortez Masto, Chair, presided in Room 3138 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada. The meeting was webcast live.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Nevada State Senator Valerie Wiener (Advisory Board Vice-Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Gregory Brower, U.S. Attorney, Department of Justice (DOJ)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Sheriff Mike Haley, Washoe County Sheriff's Office
Chris Ipsen *(Rep. for Dan Stockwell, Director, NV Dept. of Information Technology)*
Dale Norton, Nye County School District Assistant Superintendent
Nevada State Assemblywoman Peggy Pierce
Assistant Special Agent Paisley *(Rep. for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS))*
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)

ADVISORY BOARD MEMBERS ABSENT:

Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

TASK FORCE MEMBERS PRESENT:

Detective Dennis Carry, Washoe County Sheriff's Office
Lieutenant Bob Sebby, Las Vegas Metropolitan Police Department
Special Agent, Melissa McDonald, ICE

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

Nick Anthony, Legislative Counsel Bureau
Jim Lemaire, Department of Public Safety
Lynda Morrison-Rader, Nevada Department of Transportation
Ira Victor, Sierra Nevada InfraGard and Data Clone Lags

Agenda Item 1 – Call to Order - Verification of quorum

AG CORTEZ MASTO:
The meeting is called to order on October 30 at 10:06 AM.

A roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Discussion and approval of minutes from September, 2008 Advisory Board Meeting. (Discussion/Action Item)

AG CORTEZ MASTO:
The next agenda item is the discussion and approval of the minutes from the September 5th board meeting. If everyone has had a chance to take a look at the minutes, unless there are any changes, I will entertain a motion for adoption.

Motion to approve the minutes was made by Assemblywoman Pierce and seconded by Sheriff Gillespie.

Motion to approve minutes passed unanimously.

Agenda Item 3 – Report regarding Task Force Activities. (Discussion/Non-Action Item)

AG CORTEZ MASTO:
The next item is reports regarding Task Force activities from concerned agencies including the FBI, Las Vegas Metropolitan Police Department (LVMPD), US Secret Service, Attorney General's Office, Washoe County Sheriff's Office (WCSO), and ICE. Are there any reports?

RAC WHITE:
I have a number of significant cases to report. These are cases where the lab or task force had significant input and involved considerable forensic examination of computers and cell phones. These efforts either had a great deal to do with the success of the case or were entirely responsible for the success of the investigation.

I have five, but will try not to be too lengthy.

The first ICE case involved King's Buffet Chinese Restaurant in Sacramento. Most of our agents in our Reno, Sacramento, Fresno, Stockton, Redding and San Francisco offices participated. Five restaurants were involved in harboring, concealing, and trafficking of 21 undocumented workers from five different countries including China. These workers were taken into custody pursuant to search warrants. The Task Force ended up doing forensics on 8 computers taken from different restaurants and business offices. Our major concern was that these workers were being housed in very squalid conditions. Mainly, we are talking about 2 or 3 bedroom apartments and residences with as many as 15 to 20 workers crammed into small rooms that were infested with rodent droppings. Mattresses were thrown on floors. These locations were provided by restaurant owners to the workers. The Task Force played a significant part in the computer forensics.

Another case involved an individual convicted in federal court recently of coercion and enticement of a minor. Sentencing is in December. He faces 10 years to life. The Task Force was involved in 6 forensic examinations of cell phones that were used to send sexually explicit emails to eighth-grade girls in Washoe County. The girls sent nude photos of themselves to him. He posed as a 15-year old boy. He threatened and coerced them by saying, "If you don't have sex with me, I will post your photos on the Internet." An undercover sting resulted in his arrest. It looks like he will be doing some serious time.

In October, we had a case involving approximately 30 individuals, mostly citizens of El Salvador. They were involved in the MS-13 criminal gang, the Mara Salvatrucha gang. All but one of those individuals was located in the Bay Area. We did a number of search warrants over there. We ended up with one defendant, who was living in Reno. He was arrested with the involvement of Reno Police, specifically the Reno gang unit, and ICE. A search was conducted. The Task Force was involved with a computer and 7 cell phones. These are still being examined. The Reno MS-13 member was involved in the trafficking of firearms to undercover agents in Sacramento, who came from our office in San Francisco.

This was a very significant case. We had tremendous support from all the local law enforcement agencies in this area. It was very successful. The Task Force came through. It was a very long day. Often, people have the idea that the officers and agents involved in forensic examinations just sit at their desks and do nothing but exams. Believe me, that is not the case. They are out in the field a lot. They are out at 1 am in the morning. They sometimes work 24 hours a day, as needed. Many times, these cases have severe time requirements placed by courts, judges and by their own agencies to get forensic examinations completed.

We just started another case this week. It involves the trafficking of two individuals involved with a group of undocumented immigrants from Mexico. They were smuggled into the United States and brought to Los Angeles and San Jose. They worked up and down the west coast selling cheap jewelry. They worked the streets of Reno and apartment complexes as well. The smugglers worked out of a small town in Mexico. The crime lord was located there and the driver was related to him. The driver organized the smuggling into the US. He coerced them into selling the jewelry for little or no money. The standard set for the minimum amount of jewelry they were required to sell was so high that they could not meet it. For each week they failed to meet their quota, they received no pay and another week was tacked onto the amount of time they had to spend to pay off their smuggling fee. That initial fee was a six-month time period. They are being charged under 18 USC 1589, relating to forced labor and trafficking. This is the first ever case of its type on Reno.

There were 7 cell phones. The head of the organization was contacted from Reno. They were threatening the individuals with harm to their families in Mexico. They were doing strip searches of these individuals after they came back to the hotel room every night to ensure they were not hiding money or jewelry on their persons. The communications were through cell phones. That is how we were able to work the case back up the chain. We were entirely dependent on the forensics of the cell phones. The fact that we are now able to do things with cell phones we could not do before is absolutely critical. We can do much more than we could do months ago. Cell phones are really an integral part of criminal operations in this country.

We had a case in Fernley involving a 14-year old victim enticed by a 21-year old step brother to send nude photos of herself via a cell phone using a Sprint photo sharing network. That case is on-going. It looks like a good case, and will probably involve State prosecution.

The Task Force is also involved in approximately 15 interviews of suspects involved in the downloading, possession, selling (trafficking) in child pornography in this area. These are federal and State cases that are either too old or have insufficient probable cause at this point to support search warrants. Typically we go out and see if we can do consent searches and interviews to support previews of computer equipment. That may lead to actual charges. The Task Force would find that through the forensics. ICE has about 12 of these cases. There was the takedown of a server back East and hundreds of leads were sent out about people accessing child pornography. We will be following the same sort of methodology in those cases, utilizing the Task Force. We will be trying to obtain consent to search, do previews, then undertake complete forensic exams of computers to determine the existence of child pornography on those computers.

We have been very active in the past several months. Every single case we have involves technology and computer and cell phone forensics.

AG CORTEZ MASTO:
Thank you. Are there any comments or questions? Are there other reports from Task Force member agencies?

SHERIFF GILLESPIE:
Madam Chair, Lt. Bob Sebby is here with a quick overview.

LT. SEBBY:
We are currently working on 5 major cases involving, primarily, Eurasian organized crime. We are deeply involved with the Secret Service and FBI.

We have started a new undercover program where we target known skim sites. Obviously, I will keep my explanation at a minimum.

The largest thing is that over the last quarter, 69 computers, cell phones, and now, PlayStation 2s were analyzed. PlayStations are now considered computers.

AG CORTEZ MASTO:
Thank you for your report. Are the items from other agencies? Hearing none, we will move onto agenda item number 4.

Agenda Item 4 – Delegation of Authority to replace Board Administrative Assistant. (Discussion/Action Item)

AG CORTEZ MASTO:
At our last meeting, Mr. Uffelman suggested and Sheriff Gillespie, I believe, supported that the Board delegate its selection authority to the Executive Director, subject to approval by the Chair. However, the item was not an action item, so today, we placed it back on the agenda for action. I would entertain a motion if that is still the position of the Board.

> *Motion to delegate the Board's selection authority to the Executive Director, subject to approval by the Chair was made by Mr. Brower and seconded by Sheriff Gillespie.*
>
> *Motion passed unanimously*

AG CORTEZ MASTO:
We are going to take some of the agenda items out of order. We are going to go to agenda item number 7 next in order to accommodate the schedule of one of our members. I want to ensure we all have the opportunity to address legislative issues.

Agenda Item 7 (out of order) – Legislative Update (Discussion/Action Item)

SENATOR WEINER:
I have been working with Legislative drafters. I have given them the authority to work with Mr. Earl to come up with specific language. They then run that by me. Mr. Earl is engaged with these issues on a daily basis. I would ask Mr. Earl to address the issues of pre-paid cards, obtaining information from ISPs. Cyber bullying is separate bill. I would ask Mr. Earl if the other measures are incorporate in the two BDRs I have requested. If not, we should work with staff to ensure that all the concerns are addressed. He could best address that. But they are in the drafting stage. I defer to Mr. Earl on the specifics. I do review these issues periodically with staff.

AG CORTEZ MASTO:
Let us go through the various issues, starting with the criminal use of pre-paid cards. It is my understanding that representatives of my office in the Criminal Division, LVMPD, and Mr. Earl have met and produced updated legislative text. That text is now being reviewed by the Council for Prosecuting Attorneys and the District Attorney's Association. Mr. Earl, do you have anything else to report?

MR. EARL:
No, I do not. To Senator Wiener's observations, I have been working closely with members of the Legislative staff. I will continue to do so. As a matte of fact, one of the Legislative attorneys is present here in the north.

For those Board members not familiar with the legislative process, frequently, because of the time lag between when a BDR is requested and when final legislative text is drafted, as many as 6 or 7 months, it is not unusual for Legislative staff to work very closely with bill sponsors to ensure that the first text submitted to the Legislature takes account of any situational changes that may have occurred in the interim. I am doing that. It will come as no surprise to any of you who have worked with LCB staff in the past, that they are exceptionally helpful.

AG CORTEZ MASTO:
Great. Moving on to Agenda Item 7b, which is obtaining information from ISPs (Information Service Providers) and conforming NRS 193.340 to the requirements of 18 USC 2703, my understanding is that final comments have been obtained from law enforcement and minor changes will be incorporated into the final BDR text.

MR. EARL:
Madame Chair, that is correct. Let me point out that when law enforcement is involved, we attempt to get as wide participation as possible. In fact, many of the principal comments from law enforcement come from the two individuals who are most engaged, LT Sebby from LVMPD and Detective Carry from Washoe County Sheriff's Department. Both are here today. Many times when I refer to law enforcement input, a significant amount of that input comes from these two individuals, and also, from time to time, from the Sheriff's and Chiefs organization.

AG CORTEZ MASTO:
Agenda Item 7c involves records request by law enforcement from financial institutions. This involves a change to NRS 239A.150. LVMPD and the Washoe County Sheriff's Office use similar forms to request the information identified in the statute from financial institutions. This process is sometimes referred to as an "administrative subpoena." Text is being considered that would allow a financial institution's license to be suspended in the event of non-compliance. This was suggested by LVMPD in our meeting about 9 months ago. Are there any comments on this item. Hearing none, we will move on.

AG CORTEZ MASTO:
Agenda Item 7d involves student Internet safety and cyber-bullying. Possible BDR text has been submitted, as we heard, to Senator Wiener and to the LCB along the lines discussed in previous Board meetings. My understanding is that they are working on the language now.

Moving to Agenda Item 7e, credit and debit card changes, LVMPD suggested some penalties be increased for certain credit and debit card crimes. Implementing text has been provided to Senator Wiener and LCB. Initial discussions have been held with LCB staff upon their review.

Agenda Item 7f involves the encryption of personal information and changes to NRS 597.970. The encryption of business communications outside a secure environment has received considerable attention since the Board first heard from Ira Victor of Data Clone Labs several meetings ago. Nevada's law has been referenced in the Wall Street Journal, on several web sites and blogs, and has been the subject of an Executive Roundtable hosted by Code Green

Networks in Las Vegas, and a more recent web seminar by Mr. Victor. I understand that the webcast was well attended by members of the Nevada banking and retail communities. A proposal to clarify some of the problem areas in the current statute has been submitted to Senator Wiener and LCB. I understand that Mr. Victor is available to provide some insight into the reactions of various private sector interests, if the Board members are interested in hearing those reactions.

MR. VICTOR:
Thank you very much. I appreciate you taking the time to hear my feedback. I am an information security professional. I am also president of the InfraGard chapter here in northern Nevada. This is a program of the FBI to help protect the nation's critical infrastructure.

In my role as an information security professional, I have been spending the past months with "boots in the trenches", as we like to say. I have been dealing with organizations seeking to understand and comply with this statute that came into effect this month. I would like to share some of the feedback I have obtained in furtherance of clarification of areas of concern in the law.

One thing that is interesting overall is the genuine interest by many organizations in Nevada to protect this information. That is a really good sign. As someone who has been in the information security field for quite a long time, I can tell you that there used to be the sense, "We don't really need to protect this kind of information; there is not really a threat." Today, people recognize there is a threat and want to take actions to protect data. That is progress.

The fax issue does need to be clarified. I am getting questions from people about faxes. I mentioned this in my previous testimony. We have e-fax and max-fax, where faxes are converted to an email. It doesn't really get protected. The intent of the statute is to keep this information off the Internet. That purpose is defeated if a party were to send a fax out of a conventional fax machine that is then received by an e-fax into an email box, or the other way around. Some clarification on that would be helpful out there in the field.

In a similar vein, traditional faxes, from one fax machine to another, are transmitted over traditional phone lines, what is called colloquially "POTS" lines, standing for "plain old telephone service." Phone people refer to "POTS and PANS", "plain old telephone service" and "pretty amazing new stuff" – the next generation communications.

There are businesses in Nevada that use POTS lines for the transmission of credit card data to the processors. If the logic is that faxes, traditionally conveyed over POTS lines, are have a safe harbor in the law, then some clarification for traditional land lines that may be used for transmitting that data using protocols other than fax would be helpful. The challenges that businesses have in Nevada is that they have to deal with large financial services companies outside Nevada. Even if they wanted to set up equipment that would comply with the NRS, that will not work unless the other end can decrypt the transmission. While that is economically practicable when you are talking about Internet transmissions (or PANS), it is more difficult when you are talking about phone transmissions. It may make sense when traditional phone lines are involved in the transmission of data.

The other question that comes up is the definition of "business." Some government organizations say, "Well, if we are not a business, then the general public would be very upset to learn we were callous with their information." Other government agencies say, "Well, it doesn't say 'government' so we do not need to comply." Some clarification of who needs to comply with the statutory requirement makes sense. Because there is so much awareness of data theft, and information security issues overall, I think it would make sense for government agencies to step up to the plate and say, "We will treat this information as sensitive." I think citizens would be unhappy to learn that a private business on one side of Carson Street has to treat my credit card carefully, but a government agency on the other side of Carson Street does not. The public would not be happy about that.

Another clarification that would be helpful is on encryption standards. The statute is not clear on what is meant by "encryption." There is the old encryption technique, perhaps the very first ever used, called the "Caesar cipher." In antiquity, an "a" became an "l", a "b" is an "m" – just shifting the letters. If you know how many letters to shift the alphabet, then you can encode and decode the transmission. No one would consider that difficult to break. A computer could easily break more difficult encryption regimes than that. Under the statute, there really is no clarification.

Fortunately, there are standards. The National Institute of Standards and Technology, known as NIST, promulgates on-going standards that are then adopted by industry. The message essentially is, "This is the current standard we consider appropriate to keep information safe." There is a lot of confusion over which standard is good enough. I think clarification of using the NIST standard would make sense.

Finally, many people out in the field are wondering why the statute does not talk about encryption at rest. The statute currently deals with what we in the security field refer to as "encryption in transit." Using the example of a restaurant across the street from the Legislature, when my credit card gets swiped, if they are using an Internet connection, which they probably are, that data is encrypted as it is in transit to the bank processor. The data, my charge amount, a query about the amount in my bank account, and eventually, an approval code is sent back. That is encryption in transit.

Encryption at rest is actually where more of the breaches occur. We have a lot of breaches reported in the news involving various private and public entities. Almost all of them are breaches while at rest. The good news is that encryption of data at rest is becoming more common. If the restaurant across the street stores my credit card number, because I might need a credit in the future – probably not likely for a restaurant, but more likely for a hotel or a casino – they might want to store that information so that I have charges after I have left the hotel, they still have my credit card information to be able to do that. The current standard for credit card compliance, the payment card industry digital security standard, mandates that credit card data and other data associated with it like the CDD needs to be encrypted at rest. So, while it is sitting on the servers at the casino or their business partners, that data is encrypted.

The good news is that when you encrypt at rest, when you transport the data, it is encrypted too.

I have had a lot of questions from businesses and other organizations to the effect, "Ira, if we just encrypt while at rest, won't this be covered?" I reply, "Yes." But the statute doesn't really address this issue. It may be appropriate to add clarification about encryption at rest. That will not conflict with anything I see in the statute if this were to be added.

Those are the four areas of concern, the major areas, that come up. These are what I have encountered when dealing with organizations here in Nevada this month. I would be happy to take any questions from the Board based on my interactions with businesses in Nevada.

SENATOR WIENER:
I have a question. Ira, thank you for your input. We have been working on these issues for a long time together. As you have said, there is a need for more clarification than anything. As we are moving forward with the drafting of the legislation, would you be able to assist in clarifications so that we would be able to satisfactorily address these concerns. We may not have all the expertise to properly draft the clarification. If you could assist, I would appreciate it.

MR. VICTOR:
Absolutely, Senator Wiener. I would be happy to help and bring resources necessary to clarify the statute to make sense to people in Nevada.

AG CORTEZ MASTO:
Mr. Victor, let me thank you for all the assistance you have provided so far. I appreciate your continuing to help. This has been quite instrumental.

Getting back to some of the comments you just made regarding the four areas of concern, I will say that I talk to a number of national companies that work in our state and at the national level as well. Their main concern is that they want to be compliant, but, just as you said, because they are so large, it takes time for them to put together a national compliance program. I know from my conversations, it is not that they do not agree with the law, but, for larger companies, it will take time for them to comply. I just wanted to make the Board members aware of that.

Are there other comments from Board members for Mr. Victor?

SHERIFF HALEY:
Do costs related to encryption in transit emanate from a credit card company? As a follow-up, where is the cost born for encryption at rest when the movement of data may be international?

MR. VICTOR:
That is an excellent question, especially in these economic times. Businesses in Nevada are facing challenges. “Cash is King,” as they say. Businesses want to preserve cash because of lending challenges and cash flow issues.

The good news is that there are a large number of free tools available to encrypt data. I do not want to mention any one tool, for fear of sounding like endorsing it, in favor over another tool. But, businesses and governments have access to a wide variety of free tools. From a credit card perspective, credit card companies have newer terminals that use many of these encryption tools. The National Institute of Standards and Technology, for example, created a standard called AES 256, American Encryption Standard. Many pieces of free software use this standard. That’s good.

Also, there are private companies that make tools. Because of the demand, including the demand from states like Nevada – the Attorney General mentioned vendors who gave presentations down in Las Vegas – vendors are coming to the market with lower cost tools. The demand is great enough that they can have scale. The traditional ethic in information technology is there are free tools that take a little more labor to use, typically open source tools where the source code is free and open. Vendors come in and take the open source tool and add an interface that makes it really easy to set up and maintain, and their costs can be low if they have sufficient scale to be able to sell that interface to a lot of people. So, this is not necessarily a large cost.

Something else. Besides this statute, there are costs and liabilities associated with not protecting information. Many companies have had violations by now. Some government organizations have had violations as well. These tools are much less costly than not protecting the data. Both businesses and government organizations are recognizing that.

MR. ABNEY:
Mr. Victor, the last time the Board talked about this issue, we had concerns about the gap in time between the October 1, 2008 date the law went into effect, and when we can make changes in the 2009 Legislative session. Have you become aware of any issues or situations since October 1? My second question is, do we have an issue of enforcement of some of this language.

MR. VICTOR:
Thank you for that. One other issue that was brought up, although it is much lower on the list, is that there is no mention in the statute of the penalties. That is not really a concern. No one is saying to me, “Ira, there should be penalties associated with this.” So, it is not an issue of concern, but rather a question of why aren’t there penalties. I do not have an answer. That is just hanging out there in the background. I do not know whether it should be addressed or not, and have no comment on that issue.

I am not aware of any specific breaches of the law among our clients or the public generally that are more than small. The Wall Street Journal article mentioned a retailer in the Las Vegas area who receives credit card information from her customers via email. The customers email her with the credit card information in order to make a purchase. Here is what I know from experience. I do not think this has changed since October 1. In a lot of organizations, a customer will send in the credit card number and all personal information like name and billing address, expiration date, what is called the CVV number – the 3 digits on the front or back of your card – which never should be in clear text. The whole security paradigm of credit card address involves this being kept confidential – much more than the number actually. Businesses that receive that credit card have customer service representatives that hit the "Reply" button their desk top computer, and they say, "Yes, Mr. Jones, thank you for your order, it is not being processed." That credit card number now is transmitted back to the customer in the clear. So, every time you have these transmissions going two ways, you have the risk of someone intercepting them. They are intercepted. That is the nature of the Internet. It is not like a personal phone call between point A and point B. There can literally be hundreds of points in between where that data is routed. Someone who sees that data, well, it is like finding a postcard on the sidewalk. Anyone who walks by can read it.

I have not seen any large breaks with this, but I suspect there are these type of occurrences going on all the time right now.

The other data point we all should be aware of is this. Over 75% of large scale data breaches that do occur, involve someone in an outside capacity – law enforcement or otherwise – alerting the company where the breach originated. So, we would not necessarily know from the companies that it came from that there was a breach. There is just not enough time yet.

MR. IPSEN:
I would like to piggyback on what Ira is saying – specifically as it relates to State entities. As a representative of the State Information Technology Security Committee, there have been a number of requests for clarification about the meaning of the term "business". What a business is, and whether we are in compliance. We have had requests for a specific interpretation as to whether, by law, an entity has to comply. Typically we address it this way. There are a number of other standards that require us to retain data effectively encrypted. HIPPA, for example, is a federal requirement we have to adhere to. However, there is a certain amount of ambiguity among the State agencies that are requesting a formal interpretation.

Having spoken with some of the local business and counties, I think they are making varied interpretations of this as well. I concur with the need to interpret, "What is a business? What is government's role in that business?"

I also want to add to comments about encryption at the data source. That really does represent best practices. Using national standards as a reference model would allow encryption standards to change with computer capabilities. As some of the more arcane encryption algorithms become more "hackable," for lack of a better work, referencing the national standard would keep us up to date. I think all of those are excellent recommendations.

AG CORTEZ MASTO:
Thank you. Are there other questions or comments from the Board?

It is my understanding that we also may have a member of the public in Las Vegas interested in addressing the Board on this issue. I am willing to take public comments here. Is the gentleman in Las Vegas? His name is Bryce Earl. Is he present? I understand he is not present.

MR. EARL:
Before closing out this agenda item, I would like to draw your attention and that of the Board's to a letter I received electronically yesterday. Senator Wiener received the same communication from the American Electronics Association (AEA). The subject is NRS 597.970, the subject of our discussion.

I would like to summarize their concerns and then take just a minute to describe the state of play regarding BDR text. Some of the concerns the AEA identifies have already been discussed by Mr. Victor. They may also have been the subject of a seminar Mr. Bryce Earl conducted in Las Vegas earlier this month.

Moving on to the AEA letter, it begins with the recognition that there is a role for well crafted legislation. They applaud Senator Wiener and the Board for addressing the issue.

A principle concern of theirs is possible unintended consequences associated with the existing legislation. Some of the consequences they lay out are as follows. The Association's position is that the law incorrectly assumes that encryption technologies and other implementing hardware is readily available to all organizations. There is specific concern that technologies and equipment would be available to businesses in Nevada. They express concern that there is no single standard established from among various technologies, and that the area is developing so rapidly that supersession of one technology by another is a concern. The AEA also addresses the issue of financial resources, pointing out that an expenditure of funds is obviously involved to acquire and deploy necessary hardware and software to support encryption. Lastly, and this is something we have not really discussed, except in a somewhat circuitous way, the AEA points out that the standard of NRS 597.970 may be (and certainly appears to them to be) inconsistent with other provisions of Nevada statutes.

The AEA points to NRS 302A.210 requiring businesses, government agencies and other entities that maintain records containing personal information of Nevada residents to, in the words of the statute, "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use modification or disclosure." The Association thinks that is a more reasonable standard.

A moment ago, I referred to our addressing this circuitously. Both Mr. Victor and Mr. Ipsen have talked about encryption at rest. One of the issues, perhaps for us and the entire data community, is to take a look at the existing standards that appear to exist in other statutory provisions and ask ourselves whether they are sufficient, or whether it makes more sense to specifically address encryption of data as a special case. Mr. Victor has also raised the issue of whether we should look at, perhaps not during this Legislative session but in the next interim period, dealing directly with encryption while at rest.

That pretty much summarizes the letter and my initial reaction to it. I also received a communication from Microsoft that noted its approval of the AEA letter. Both organizations indicated a willingness to provide further information and to participate on behalf of their communities of interest.

The AEA letter responds to the law as it is, and does not take account of some of the changes that have been proposed in the BDR presently in the works. After Ira's initial presentation to the Board, Ira, Jim Elste, previously of the Department of Information Technology and now heading information security at IGT, and I spent time together. We came up with draft modifications, as the Chair has indicated, to Senator Wiener and LCB. Senator Wiener has graciously consented to sharing that proposed change with other members of the technology community and interested members of the public. We have done that in the past, and have received some input back. Some of this information is the basis for some of Mr. Victor's observations this morning.

One of the things I propose and intend to do is to get back to AEA and Microsoft with the text of the BDR changes presently being considered. I would ask that they respond to those changes, so, they would not be responding to the law as it exists, but to the changes some of us have identified as making sense.

In layman's terms, the present proposed BDR text would establish a safe harbor. It would essentially say to the business community that if you use the following type of encryption, either open source or standardized methodologies, then, should a data breach occur for data in transit, your liability for that breach would be limited in the following way. The idea behind crafting a change designed that way is to provide an incentive to businesses to employ standardized methods of encryption, and to do that in a way that would largely be self-enforcing. As a result, it would not be necessary to consider criminal penalties or to establish a regulatory regime to oversee implementation. Rather, the safe harbor provision in the statute itself would provide an incentive to businesses to adopt existing technologies in order to meet a very basic encryption requirement.

That describes the text that LCB, Mr. Victor, others, and I are working with. I would like to share that with AEA, Microsoft and with other interested businesses.

AG CORTEZ MASTO:
Thank you, Mr. Earl. Are there comments from the Board members? Hearing none, are there any other issues connected with the Legislature we did not cover?

MR. EARL:
Madam Chair, I do not know of any. I put that in as an agenda item because Board members' memories may be better than mine.

AG CORTEZ MASTO:
OK then. Thank you, Mr. Victor. We will go back to the original order of agenda items.

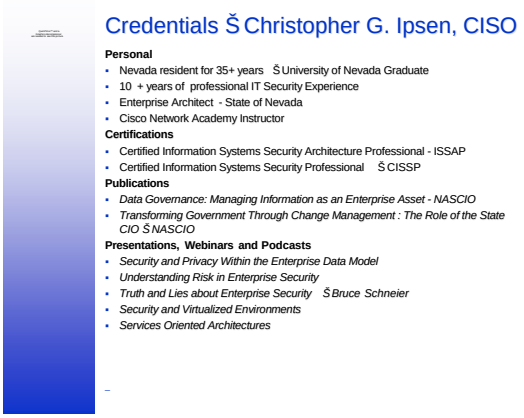
Agenda Item 5 – Presentation by Chris Ipsen, Chief Information Security Officer, Department of Information Technology, Security Challenges Facing the State Systems and Assets, Current Actions, Future Proposals and Role of the Tech Crime Advisory Board. (Discussion/Action Item)

AG CORTEZ MASTO:
As you know, one of the Board's statutory missions is to "assist the Department of Information Technology in securing governmental information systems against illegal intrusions and other criminal activities." With that in mind, I look forward to hearing what Mr. Ipsen has to say.

MR. IPSEN:
Thank you, Madam Chair. Before I begin my presentation, I want to take a second to say what a privilege it is to sit here. I was sitting with my children last night talking about what you do for a living. If you can not capture information security in terms you can explain to your children and the people around you, well, security in obscurity is non-existent. I took a second to explain to them how privileged I feel to sit here with all of you, having listened to all of your presentations. I want to express how genuinely dedicated I expect us to be regarding protection of citizens' data and identities moving forward. The title of my presentation is, as you see, "Security … a business enabler."

This is not intended to be an IT (information technology) presentation. Although, in my world, I have to live with schemes of encryption, key management, different methodologies for multi-tiered security models. This can become very complex very fast when dealing with separation of duties.

My goal is to present this subject in a business sense. I should be able to communicate to all of you. Ultimately, my goal is to engage you in a collaborative cooperation to move forward to protect the citizens' data. That is the focus of our office. What do we need to do to protect citizen information.



I am a Nevada resident. I list that first on my slide.[1] I have lived here for 35 years. I attended the University of Nevada. It is very important to me to have seen Nevada grow to where we are now. Previous to my current position, I held the role of Enterprise Architect of the State. This blends IT capacity and business capacity for State systems. Before that, I was an instructor at a number of different levels. My certifications and presentations are not nearly as important as the necessity to convey how security fits into the overall scheme of businesses in the State of Nevada.

I hope to give you a brief idea of what is out there. We all know it is scary. I want to give a couple of representative examples in a benign way and talk about our State infrastructure. We can not get too granular into what we have. I want to speak to some of the risks and liabilities the State has whether we choose to accept them or not. In most cases, State employees, very similar to the private sector, do want to do the right thing. We need to be able to capture this risk analysis in a business context so that we can apply appropriate resources to securing the need.

In these fiscally constrained times, it is very important to capture potential liability and also the capacities and responsibilities we have moving forward to protect the citizens' data. I want to talk about two things the Office of Information Security does. I would be glad to come back and talk in more depth at a future time. This is a brief overview. At the end, I want to focus on what opportunities we have to work in a collaborative sense to meet some of these challenges that face the IT departments, the data, the citizens. I want to focus on our business expertise. Without all of us working together, we do not have a security model for the State.

We face a number of different threats. From the outside, we see things change. It used to be that people would hack into systems for glory. "Look at me, I am really smart." That has changed. Sovereign nations are now involved with concerted computer hacking. Business entities, as we know, are focused on stealing our data because there is a profit motive. There are a number of politically motivated attacks that influence behavior. Some of the targets, if affected at the right time, can be very detrimental to world economies. I have an example where that occurred recently.

There are internal threats that are both intentional and accidental. People with privileged access to data can use that access in a detrimental way if they deem it necessary. Separation of duties – understanding that there are internal risks – is very important.

There are inherent vulnerabilities in software, systems, and mobile devices. Everything that enables us to do business better also exposes data to greater risks because the data becomes more mobile. Data becomes more ubiquitous in our system. If there are constraints on the confidentiality of that data, there can be real challenges for the State and for businesses.

Lastly, talking about motivations, it is changing. We are no longer only dealing with social misfits. It is very organized, with an associated profit motive.

[1] Not all slides presented to the Board are included in these minutes.

An example of this is the World Bank. Just recently, in July of this year, the World Bank was compromised. Without getting into the specifics, I took a brief excerpt from the memo of the Information Security Manager for the World Bank. The World Bank is in charge of the International Monetary Fund, which funds entities in times of need. When we have times, as now, where funds are very constrained, disruption of service at the World Bank can be a very significant event. What is important here is the types of services that were compromised.

I highlighted three servers. One is the domain controller. It allows you to access all resources on a network. This is a pretty significant compromise. The second is the certificate server. We have talked about encryption. Enterprise encryption relies upon key management and certificates. This is their encryption server. Having an encryption server means that their encryption is no longer effective. Lastly, was their secure ID server, their identity server.

What does this mean? It means that who ever hacked this system now owns everything. The most recent data indicates that, most likely, the hacking came from a contractor, who left an open door at some point. The data streams associated with the compromises originated from China. The significance of the understanding of China to control this infrastructure, well, you can infer what you want, but this is a very significant event. It is not uncommon for a target like a State to be similarly challenged.

Turning to an example of an internal threat, last July, the city of San Francisco was, and to a certain extent, continues to be held at bay by a single individual, who had ubiquitous access to the city's IT transport network. This was a senior manager within the system. His scheme was very complex and self-designed. When challenged by city officials to provide the keys he used to access the over 1100 devices on the network, he refused to give up that information. One individual was able to hold the city at bay. He went to jail. He is still in jail with a $5 million bail. Mayor Gavin Newsom had to go to the jail at midnight to plead with him to provide the key information because of the potential liability associated with owning the entire network. The city has now set aside $1 million to analyze the network to ensure it is secure for the continuation of city business. The total cost remains unknown. This is an example of a situation where internal duties were not separated.

When we consider inherent vulnerabilities, the question revolves around data. How many people have privileged access to data? Can it be mailed out? Can it be received inbound? Those things that make us effective, also present challenges. Mobile devices like this Blackberry have the capability of holding 4 GB of data. If I have access, I can carry this our with me. There are thousands of USB drives. They may cost only $5 now – sometimes they are free if you position yourself right. A portable device that may hold 5, 10, or 20 GB of data – that is a significant amount of data within the State system.

Software vulnerabilities are another concern. Weekly, as members of the U.S. CERT pool and the multi-state ISAC, we get Microsoft advisories identifying remote code execution vulnerabilities. This sounds benign. Here is what it means. Someone on the wrong side can end up owning your machine. If you are on the inside of your network and they own your machine, then they own what you can access. This is very frightening.

The State has hundreds of geographically dispersed subnets. If you think of the State, think of every single city and municipality. We are represented in all of these locations.

Finally, we have a number of compliance regulations. Echoing Ira's testimony, we should be addressing this. Senator Wiener, thank you very much for addressing this encryption necessity. We need methodologies for controlling this data. Compliance plays directly into this need.

We know the threats are large. We know that they come at us from every angle, whether inside or outside, whether from software or elsewhere. What is our State infrastructure?

Without getting into the specifics, let me give you and idea of what I see every day. We hold information on all identities represented within the State. If you look at DETR, the Nevada Department of Employment, Training and Rehabilitation, you find records of everyone who has ever worked in the State. DMV, Department of Motor Vehicles, has records of everyone who has ever had a driver's license. How about the Department of Health, which maintains data on birth and deaths and so forth? We probably have a 3x magnifier of all the people who ever resided in the State or work or have businesses. We have millions of identities. We will look at that in a risk scenario.

We probably have 3600 different data applications in use by the State. We have data that flows up from the counties and on to the federal government. We are an intermediary for all government entities within the State. We have millions of records that are transmitted for reasons of compliance with federal requirements. Our communications infrastructure has hundreds, if not thousands, of routers and switches. They are in every geographic location. We have over 18,000 employees. This is important when we consider the internal threat and privileged access. In addition, we utilize many secondary contractors and subordinate employees of counties and cities. We spread this out over a large geographic area.

Hopefully, you now feel a little uncomfortable. My goal is to say, here is the challenge and here is the infrastructure. We can not leave it there. The real question is, "What do we do with this?" The key is to develop an effective risk management strategy. This must encompass both the protection of the data and the identities. It must also maintain the availability of the infrastructure. We have a business need for the State, especially in times of emergency, to remain resilient. How do we provide the necessary services citizens expect. In understanding this, we have to understand that an individual identity could potentially cost the State $200 – the going rate for identity theft. We have 10 million identities. How much should we spend, what should we do legislatively or cooperatively, to protect the data? We know what the risk model is.

The Office of Information Security is a relatively small, but significant, office within the State. We have approximately 10 employees that work with all State agencies. Our goal is to enhance the capabilities of every entity within the State and to work collaboratively with each of the department ISOs (Information Security Officers) to achieve a certain set of standards. The Office of Information Security is actively engaged in a process, known as the information security life cycle. We assess the posture of the State. We protect the data of the State. We monitor for compliance. When we see something wrong, we address it.

We do security assessments, not necessarily for forensic or criminal purposes, but for State civil purposes that fall outside criminal activities. We do technical vulnerability assessments. We do physical security assessments.

To protect data, we develop policy, standards, and procedures. Later, you will see that, as of last month, we were able to complete a consolidated, easy-to-read security policy for the State. This was a huge effort. We have had policies before, but, now, we were able to combine them into one document that is easy for entities to use.

We engage in the field of technical security architecture. Also, and this is an important, but often overlooked area, we engage in security awareness and training. We have 18,000 employees. Each represents a point of potential failure in the system. We need to communicate to them what they should be doing. We are engaged in automating that process because we are so decimated in our ability to rehire people.

We monitor the State infrastructure. More importantly, our office audits the people who are monitoring the system. We have separation of duties in many key areas. Recently, without any specifics, we were hit internally in a situation where duties were not sufficiently separated. We address that as well.

We have intrusion detection systems and intrusion prevention systems. We oversee the correlation of these attacks. We look at log files that should exist in an attack, and we respond. We have computer incident response teams. If we know a hack has occurred, agencies have a legal responsibility to report it, and we have a legislatively-dictated responsibility to address how and what happened, and are appropriate procedures in place to address future known vulnerabilities.

A subset of our concerns is continuity of operations in a disaster – the implementation of a disaster recovery plan. We also do administrative security investigations.

What is the State response? What have we done? We have a highly effective, and by that I mean a near tier 3 data center. If you have the chance, I would like to extend an invitation to the entire Board to visit the State data center. It is an excellent operation. It has multiple layers of redundancy and security. The citizens have paid for it, and I invite you to tour it.

As I mentioned, we have developed a consolidated State security policy. I have copies of that, and I will bring some the next time we meet. We are printing it as we speak. I would like to provide that to all of you so you can see what a policy looks like, what standard looks like, and what a procedure looks like. There are formal national standards describing how data should be handled. We are aligning our State practices with industry best practices. So, the ISO 27002 standard for handling data and security is what we are aligning with. We are not inventing our own standard, rather we are using what the private and public sectors have collectively identified as best practices.

The Department of Information Technology has developed standards that map to those policies. What does this mean? With the exception of two or three remaining policies, our policies have standards built so that an agency without them, perhaps Health and Human Services, or NDOT, can easily adopt the standards we created. The standards are specifically written so that the "Department of Information Technology" can be erased, and the name of whatever agency

adopting the standards can be inserted. We are trying to enable the agencies by making their standards as effective as possible.

The fourth issue, which I believe is really important, is working with the Attorney General's Office, we standardized and coordinated our responses to security incidents. What does this mean? Often, we are called in to deal with an administrative problem within an agency. Let's say they have prohibitions and penalties that say an employee can not surf the Internet looking for pornography. An adult looking for pornography is not against the law. It is against State regulations. That is when we would be called in.

Let's say we are called in. We do a forensic analysis of a computer to determine whether an employee has indeed done what has been asserted by management within the organization. We are an independent party. We are not part of their administration. So, we can take an objective view. Let's say we find something that represents criminal activity, for example, child pornography on a computer. With our old policies and procedures, and our lack of funding for forensic tools, we could potentially disrupt a case before handing it over to the Attorney General. Rather than doing something good, we might do something that would hinder the law enforcement effort. We have now aligned ourselves with the investigators in the Attorney General's Office. We have showed them our policies and procedures. We have asked for an internal review from the investigators. Our primary concern is, based on what we see on the computer, if there is something there that exceeds our mandate, we hand it off to the Attorney General. So, we now have a continuation and continuity of process so we do not disrupt what eventually could become a very significant event. I think this is a good demonstration of how well cooperation can work.

We are in the process of automating our security based line of servers. There are a number of tools. I wish we had the Cadillac systems, but we do not have the money right now. We are building our own scripts. We are looking at going out and analyzing every one of the hundreds of servers in our data center for known security vulnerabilities. This is a daunting task. What do you with the data after you get it off? We are working on how to communicate that to the local administrators.

We have on line security awareness. Yesterday we were asked to assemble some modules that were specific to IT personnel – not general users – to identify best practices for them.

This is a "Top Ten" list, now a "Top Twelve" list after our security committee meeting yesterday. It talks about where our opportunities are in security initiatives. Note that number 1 is encryption. Ira stole a bit of my thunder. We, in the State, need to get a grasp on this, and we need executive sponsorship, moving forward. Even though there are free tools, developing an effective encryption in an enterprise can have costs. There are costs in the keys that encrypt the data and the processes. We do require resources and training for this.

Turning to data lost prevention, how do we validate that data has not been lost? What if someone comes to us and asks, "What did you do with my data? I saw it out on the Internet." If we believe the data did not come from us, how do we validate that?

There are tools available that need to be addressed to ensure we are doing everything we can to protect the identities and data of the citizens of the State.

Centralized e-discovery is a huge issue that branches into multiple areas. The Attorney General's Office certainly has a role here to determine what the legal requirements for retaining data are and what the discovery requirements are that are associated with public records. It makes no difference whether we are talking about emails or text messages or paper communications of some sort. This problem is huge. NDOT has millions of records. Health and Human Services has millions of records. If the State does not get a grip on this, there are billions of dollars of liability if we do not have the records necessary moving forward. We need some methodology that incorporates our State records manager, who has the ability to define what a record is and what is not, and what the retention schedules are with the electronics record committee. IT personnel need a physical way to manage the requirements, whatever the legal requirements are.

When agencies come to me and ask, "What is our legal requirement for data at rest encryption?" I want to be able to say, we will talk to the Attorney General's Office in order to get a standardized response to all agencies so they can comment and have an understanding of what that is.

I could spend several sessions with you talking about identity management. There are huge opportunities here. Uniquely identifying an individual and ensuring they have the rights to access particular data that may be theirs is absolutely critical.

An actionable business continuity plan is important. This was demonstrated recently in Texas. IBM was working as a contractor for the state. It was not backing up the Texas data. A $900 thousand dollar fine involves the agency. All of their outsourcing efforts are now on hold as the result of problems with this $860 million contract. In order to ensure we have usable data, it is not just a question of backing up the data, but also making sure you have the capacity to use the data once you have accessed it again in an emergency.

We also need enhanced on-line awareness that is specific to the needs we have. We have thousands of people. Obviously we are unable to talk to each individual. We need to build modules for State employees and people who work with records, so we can communicate and validate they have undergone the necessary training. This is a huge undertaking, but it is something we need to do.

You will see a number of other issues, in black on the slide. These are equally important, but the items in red are items we need to address immediately.

Improved mobile device management is a problem. With encryption, we might be able to achieve that.

We need improved data classification. What is confidential and what is not? If you have millions of records and can not answer that question, how do you validate that you have protected the data? As a State, we are open, we need to make our records open and available where appropriate. However, when it comes to an individual's personal data we have required them to give to us, for example, when my son was born 9 months ago, he had blood tests and the results were required by the State, how do we exercise our fiduciary responsibility to protect data like this. I believe if we are requiring citizens to give us their personal information, we have a responsibility to protect it. To protect it, we have to be able to identify it. That is were discrete methodologies for classifying data, although very cumbersome and difficult to do, needs to be done.

Moving on to improved web-based application security, this involves an emerging threat. I do not want to belabor it. There are all sort of scripting problems. Just go to a web site as a user, you can be compromised. A user's data can be redirected to another site. Presently, there are no good methodologies other than some web application firewalls and forensic tools to prevent this from happening. This is a major problem. I will be glad to talk about this more in the future by bringing in industry experts in this area.

We need an adaptive security model for emerging technologies. As we move forward, the State is looking for ways to save money. We are embracing emerging technologies, like virtualization. We need to have security models that adapt to those business practices so that we can capture the benefits of these emerging technologies. If it doesn't work, or if it is not secure, the State can not use it, despite potential cost saving advantages. So, security here is a major point.

The last points on the slide, 11 and 12, were added by the Security Committee. They asked, "Please put these in." Technical security training for IT personnel in government agencies and departments is something the IT managers said they would love to be able to do, but they have other jobs too. There are very few dedicated information security offices even within large agencies. The only two or three major agencies that a single (one!) dedicated ISO are Public Safety, NDOT, and Health and Human Services. These agencies probably represent 80% of the State. They can not do it all. Security training for IT professionals, for all of the different aspects is very important.

As we start to move towards integrating systems, secure internal file technology becomes important because we need to be able to move information securely.

The next slide showing collaborative opportunities is very important to me. From an enterprise architecture standpoint, if we do not work together, we will have no security. There is no security in a silo design.

One of the things I would like to ask for is a dedicated attorney general for the Information Security Committee to help us work through some of the legal requirements associated with the business practices that we entertain. Secondly, we need executive sponsorship for key information security initiatives. If we can capture what they are, we need support from Board members like Senator Wiener. Without sponsorship we do not have much possibility of getting many of these things achieved. We need legislative support for key information security initiatives. Last, we need increased visibility for information security programs. If we can do that, I believe we can get a handle on some of these difficult and challenging problems that face the State.

Hopefully, I have not taken too much time. These concerns are very large. They need to be addressed in an effective business fashion. I will be glad to entertain questions. I am also available any time on any of these issues.

AG CORTEZ MASTO:
Thank you very much, Mr. Ipsen. Are there any questions or comments from the Board? I will say this. It is apparent from your enthusiasm and the information you have provided to us, that DoIT has the right man for the job. Thank you again for your presentation.

MR. IPSEN:
Thank you again for the opportunity. I really do consider it a privilege.

Agenda Item 6 – Presentation by Detective Dennis Carry, Washoe County Sheriff's Office, On-line Challenges facing Nevada Law Enforcement (Discussion/Action Item)

AG CORTEZ MASTO:
Agenda Item 6 is a presentation by Detective Dennis Carry. My understanding is that Detective Carry of the Washoe County Sheriff's Office is that he has been active in the Internet Crimes Against Children (ICAC) task force for several years. We look forward to your presentation.

While Detective Carry is setting up, let's move on to Agenda Item 8.

Agenda Item 8 – Possible Board and Members' tracking of items of legislative interest (Discussion/Action Item)

MR. EARL:
During the last legislative session, Board members agreed to assist one another in tracking bills of interest. The Attorney General's Office, the Banking Association and I exchanged informational lists of bills we were interested. I would certainly be willing to facilitate a similar exchange this year. If individual Board members were interested, I would provide copies of those exchanges to them as well. Keith Munro of the AGO and Lt. Roberts of LVMPD and I have already had discussions about what bills are of joint interests. I will be willing to facilitate any type of collaboration before and during the session.

SHERIFF HALEY:
Mr. Earl, would you please add Lt. Tim Kuzanek to your list. He represents my office during Legislative session.

AG CORTEZ:
If there is nothing further, and we are still setting up, let's move on to Agenda Item 9, which is Board comments.

Agenda Item 8 – Board Comments (Discussion/non-Action Item)

AG CORTEZ:
Are there comments from the Board at this time? Hearing none, let's move to Agenda Item 11, scheduling of future meetings.

Agenda Item 11 – Scheduling future meetings (1st quarter of 2009 during Legislative session) (Discussion/non-Action Item)

AG CORTEZ:
Last session, Board Legislators indicated a preference for a meeting during the first several weeks of the session. This scheduling would maximize the likelihood of their attendance. If this remains the case, are there particular days that might be better than others? Since the Legislative facilities will be unavailable, we will likely meet in the Mock Courtroom in the Attorney General's Office in the north and in the Grant Sawyer Building in the south. Mr. Earl?

MR. EARL:
I take it that Senator Wiener has left. Assemblywoman Pierce, without putting you unduly on the spot, are there particular days or weeks that would likely appeal to you and Senator Wiener. If nothing immediately comes to mind, I would be glad to work with you informally to maximize the possibility of getting as many Board members present during what is likely to be a fairly tumultuous time during the first part of the next Legislative session.

ASSEMBLYWOMAN PIERCE:
We should probably stay away from Mondays and Fridays. This is what comes to mind immediately. It will be difficult.

AG CORTEZ:
That is helpful. As the session starts, we will try to work around the schedules and coordinate with both you and Senator Wiener.

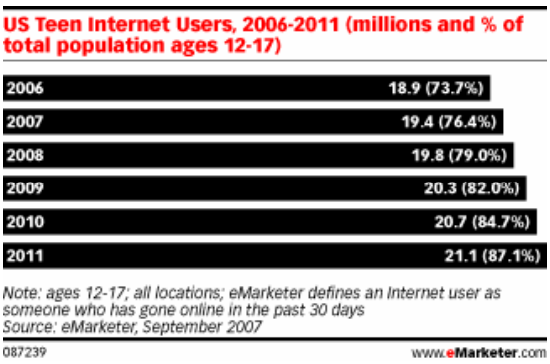
I think we are about set with the projector, so let's move back to Agenda Item 6.

Agenda Item 6 [Continued] – Presentation by Detective Dennis Carry, Washoe County Sheriff's Office, On-line Challenges facing Nevada Law Enforcement (Discussion/Action Item)

DETECTIVE CARRY:
Thank you Attorney General. I am not going to give a very long presentation. Part of the presentation involves Second Life, which was discussed by Lt. Cohen during the Board's last meeting.

I am going to address some issues of how Second Life will impact Nevada, as well as how it will affect our laws.[2]

I am Dennis Carry, a detective of the Washoe County Sheriff's Office. I work with the ICAC task force as well as with the FBI's Innocent Images task force. I have been a detective for just over 5 years and with law enforcement for over 12 years. I also conduct computer forensics, so I am well aware of how that aspect impacts law enforcement in the State.



You are all aware, as members of the Tech Crime Advisory Board, how technology is rapidly expanding. It will affect everything going on. The Internet is expanding faster than anything right now. World wide estimates of Internet users are at almost 1.5 billion users. In Europe alone, there are over 384 million users. North America has almost 250 million Internet users. These numbers are estimates from this year. The United States alone has nearly 220 million Internet users. This is a 13.5 million user increase from last year. This represents nearly 72% of the U.S. population.

The Internet growth between 2000 and 2008 is over 130% measured by users. When considering how many Internet users there are, we tell people to look at their own households to see how many computers they have, how many kids have their own laptop, how many friends come over to use your Internet connections. There are a lot of connected people out there.

This graph, produced by eMarketer, shows U.S. teen Internet users between 2006 and 2011. Most of these numbers are estimates based on their surveys. In 2006, they were estimating teens between 12 and 17 years old numbered about 18.9 million users in the U.S. This year alone, the estimate is 19.8 million, but by 2011, estimates are a total of about 21.1 million U.S teens between 12 and 17 will be on the Internet. I think the reality is that we will see more than that.

[2] Not all slides presented to the Board are included in these minutes. The background of Detective Carry's slides has been changed.

Computer and Internet use are growing because the cost of computers is going down so much. Right now, you can go to Wal-Mart, spend $300 and get a great computer. Because prices are going down, use is growing.

Why is the Internet widely used? There are computers in most homes today. Growing up in the technology age means computers have jumped leaps and bounds since the 1980s. Twelve or thirteen years ago, the average computer was about $1200. Now it is $300. Most children aged 12 and up are given school assignments that require Internet use. In fact, in many schools, homework assignments are not given in class, but posted on the Internet. So, students are required to use the Internet.

Newspaper sales have dropped and the Internet affords instant access to information, news and shopping. Right now, you can go online to CNN and know the news before most public safety or other government officials because it is being reported there instantly.

Virtually everyone uses some form of email or goes on line to find out what times movies are playing. The Internet has also become huge for pornography, both adult, and unfortunately, child pornography. Why is that? Because someone can sit at home and use it discreetly.

The Internet evolution of child exploitation is the next topic I will talk about briefly. Enticement or luring is when someone contacts a child or juvenile via the Internet, either through email or instant messaging, to try to lure them to do something. Child prostitution has evolved from pre-Internet to now. The child sales trade involves the selling of children on the Internet.

Prior to the Internet, child pornography was sent through the mail. There was an underground, black market. It was more difficult to get. Much came from overseas. There were collectors that would somehow advertise it was available, usually using code words in other forms of advertising.

Child sexual exploitation such as pornography, prostitution, slavery and so on, would be advertised in classifieds, underground clubs, and, maybe adult pornography stores using code words. People had to know exactly what to look for. In the old days, “perverts” wandered around in trench coats using accidental touching and voyeurism. That is the general public perception of what a pedophile or pervert or some one who would harm a child would do. They thought they could spot them because they would be dressed in a trench coat in a park. We all know that just is not factual.

The current trends of online exploitation involve Internet chat rooms and instant messaging. Everyone has heard of Yahoo instant messaging, or AOL Aim, or other forms of instant messaging. A few years ago that was a big thing. No longer. Today, virtually every teenager has a cell phone and they text each other back and forth. They still do instant messaging, but not at the level that it once was.

Now they are using online gaming. In online gaming, you can talk to other people that are playing the same game. You can sit at home, play an online game on X-Box or PlayStation, and be playing with people in Hong Kong, or any other country in the world. You can communicate with them in real time.

We know about social networking sites. MySpace and Face Book, the most popular right now, are among many others that are out there. Virtually every teenager is on there now. Even if they do not have a computer at home, they have gone to someone’s house to get onto these sites. They can go online through their cell phone to create a profile on a social networking site. As we know, the Internet predators, the people we need to look out for, are out there at the same time. Internet Relay Chat (IRC) is not very common in this area right now. In the past, people used to collect child pornography through a Internet news group, where photos would be emailed throughout the group. It still happens, but is no longer so prominent.

Then there are underground or foreign web sites. Most child pornography web sites we come across seem to be based in other countries. When they are based in the United States, they are taken down quickly and they are aggressively prosecuted. But, they are still out there. Some countries do not take care of this problem.

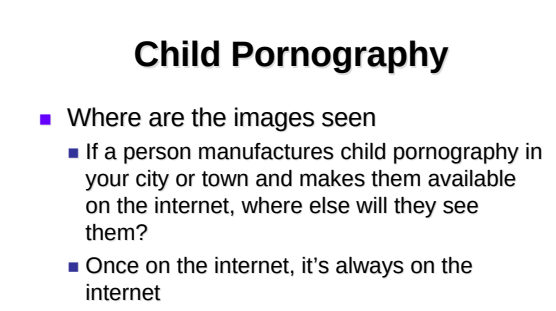
We need to think about where the images of child pornography are seen. If a person manufacturers child pornography in our city or town, or your city or town, and are made available on the Internet, where else will they be seen?

The general public does not understand the severity of this. They also do not understand that once a picture is on the Internet, it is always there. It is going to be there forever. It will be passed around from one person to the next.

This is called continual exploitation. I am going to show you a quick video.

AG CORTEZ MASTO:
Is this something that is appropriate to be aired since we are webcasting?

DETECTIVE CARRY:
It is not child pornography. I am having some technical difficulty, but what it shows is how an image spreads across the world. The tracking shows the spread of an image of a real child. It has been tracked through various ICAC task forces, the National Center for Missing and Exploited Children, Interpol, and other government agencies involved in tracking child exploitation.



The video shows a map of how rapidly this one image of one child went from one place in the world to all around the world in a two-year period. Essentially you will see a map of the world. You will see green dots that represent where we know this picture has been viewed, recovered, or seen by somebody. Eventually, the entire world is blanketed in green dots. That is within a two-year period. We show this video to emphasize how quickly this spreads. Lots of prosecutors, judges, law enforcement, and citizens thinks that a person merely got an image, perhaps from someone on the Internet. They do not put this in personal terms – that could be their daughter, and her image could be all over the world and always will be.

Where do we find child pornography on the Internet today? We find it in peer-to-peer networks that share files. Some of these networks are Lime Wire, Fair Share, and Causa. There are many of these networks. People also use these networks to trade songs, legally or illegally. They trade videos as well. It has become such a problem that now you can go onto a peer-to-peer network, type in a word you know will bring back child pornography. All you do then is download the movie or video. You can have it within minutes.

As I mentioned, you can obtain child pornography through news groups or email it back and forth. You can also get child pornography through websites – usually pay websites. These can be the subjects of very large take down operations because someone had to use a credit card, whether it was theirs or one that was stolen. There are free websites. These are predominately in other countries. Sometimes it is hard to find a child pornography web site unless someone reports it. The only way it is reported is if someone accidently ends up on the site, or if someone was caught while visiting it. The offenders will not report it unless there is something really strange that proved to be too gruesome even for them. Shockingly, that does occur sometimes. They will report something they thought was tasteless.

At the last Advisory Board meeting, Lt. Cohen gave a quick virtual world presentation. It is becoming the future. Crimes are moving to virtual worlds as well. Child pornography will increasingly be passed through virtual world sites. Enticing and traveler cases will occur there. Endangerment cases, cyber bullying, harassment, terrorist threats, hate crimes, fraud cases, file trading, viruses, Identity Theft – everything will be occurring in virtual worlds.

Second Life, introduced at the last Board meeting by Lt. Cohen, is an online virtual world that uses avatars – images of people created and dressed by people however they want. Avatars represent people and people can communicate through their avatars. You speak through a microphone or type something at a keyboard and the other avatar, the other character, is seeing what you are typing. Avatars can invite one another to watch movies or join group meetings.

Let me show you the Second Life introduction.

VIDEO VOICE:
This video is machinima, video film in Second Life, a virtual world. I am going to explain to you about Second Life and many of the companies that are using it to their advantage. Second Life is an immersive, 3-D virtual world. Users control their avatars to create content and their own in-world experience – used to create their own lists of friends and to join or create groups. They communicate with other avatars by a track of instant messaging. Users in Second Life own the intellectual property of whatever they build. They can also buy and sell objects with real money. Second Life has its own currency of Linden dollars and a foreign exchange called Lindex. The Linden dollar trades against U.S. dollars. There is a social network in place. Users in Second Life can meet friends from the real world and have discussions, debates, and transactions. Innovative businesses are starting to explore the potential of these new worlds. Durand Durand is setting up a band community island to be opened in the near future. Warner Brothers is promoting a new movie in a New York styled loft.

DETECTIVE CARRY:
For the sake of time, I am not going to play the whole video. As you saw, there were a group of avatars that were joined around in front of a big movies screen. We will talk about this issue shortly.

This is relatively new. You can imagine what Second Life will look like as technology advances. It will look no different from the television shows over the past few years where people put on virtual goggles and they can move things on screens by moving their hands. That will happen.

AG CORTEZ MASTO:
Let me ask a question. Is Second Life the only type of virtual world? Are there others?

DETECTIVE CARRY:
Second Life is one type. It is one company, Linden Labs. It is free, although to get the most benefit from it, you have to pay. There are other virtual words coming out, and we are about to see an up and coming one. Just like MySpace used to be the big thing, and now Face Book has taken over, other social networking sites know that where there is money, there is opportunity. Companies will start building on this.

In a virtual world, you can buy property, a house, clothes, jewelry, and dress your character as you want. You can make friends, visit clubs, dance, flirt, and join a variety of groups – anything you feel appealing or interesting. This is happening with hate crimes too. We have groups that are going to Second Life and other virtual worlds to have their meetings. You can get a job, and, in some cases, even quit your real job because you can turn it into a profitable money making venture inside Second Life because Linden dollars convert to real dollars. There are over $1.5 million a day in transactions in Second Life currently. You can buy weapons, or anything else, and have it shipped to you.

Education institutions have caught on to the opportunities in virtual worlds. They are teaching in Second Life and most virtual worlds. Children in most school districts, if they are absent a certain number of days, run the risk of not passing and having to repeat the grade. Why can't a sick session go online and view the class, just like people are viewing this session from their home or office. It is going to happen. Perhaps schools of the future will not be built as they are today. Perhaps they will be based on everyone having a computer at their house.

Imagine holding meetings with people world-wide. Many businesses have bought into Second Life to have their meetings. Why pay money to fly a client to the United States from Japan, when you can go on line. This may be better than video conferencing because someone can actually see the product and take part rather than just seeing it on screen.

The Advisory Board could have its meetings through Second Life. Congress, state legislators, everyone, could conduct their meetings through Second Life or other virtual worlds.

What are the concerns though? Imagine a terrorist briefing in a room online, where only invited avatars could take part. For example, a group of terrorists could meet in Second Life in a private room. Other people can not go in and see what they are doing. It is like a telephone, only it is occurring over the Internet, maybe with a broadband connection, maybe cellular Internet, maybe dial-up Internet. Do we have the ability and the resources to go in and police that area? I will tell you right now that we really do not. Maybe some federal entities have that ability. We do not.

What are the concerns?

- Imagine a Terrorist briefing in a room online where only invited avatars can take part.
- Imagine a pedophile group meeting discussing where to find victims and what to do with them.
- Imagine gangs and other criminals discussing in a virtual world how to organize, recruit, and commit crimes.

Imagine a pedophile group meeting to discuss victims and what to do with them. Imagine gangs and other groups discussing, in a virtual world, how to organize, recruit, and commit crimes

This video shows how to create a video on your own land in Second Life. You basically draw a box and stream whatever video you want to play in it. We will skip the movie for the sake of time.

This is a concern because someone can create a movie screen and stream child pornography to anyone they invite to come watch it in Second Life. Maybe we will not know it is there. We might not be able to know. We might never find evidence it is occurring.

Sony is coming out with its own virtual world. It was scheduled for release earlier, but has not come out yet. It will be used with Sony PlayStations. The Sony PlayStations are more powerful for graphics than most computers. As a result, the graphics in a virtual world will be far more advanced. It is expected to rival Second Life.

One thing you can do in a virtual world, particularly the Sony virtual world if it ever takes off, is this. Imagine walking past an avatar, your character is walking past another character. As you move closer, you can hear this character talking to another character just like real life. As you stand next to them, you hear them, just like you are standing next to them in real life. As you walk away the sound of the conversation diminishes. That will create some problems. As a police officer, I can record people I am talking to. I can have a tape recorder on. I do not know what I can do in a virtual world, because it has not been addressed yet.

What if you create your own apartment in a virtual world and furnish it as you want. How would a child pornographer furnish his own virtual apartment? What if the wall paper consists of virtual

child pornography images? What if the large screen television shows child pornography movies? What if the offender is brutally raping a child and live-streaming the video to anyone invited to come into that private room and watch?

My concern is that I know this will happen.

The problems we face on line right now, whether in virtual worlds, child pornography, or anything to do with online crimes, are problems that many investigators and first responders are not trained to identify. They do not know Internet sexual exploitation when they see it many times. Many children do not report incidents of online exploitation. Children typically will not report unless something really bad happens to them.

Prosecutors are seldom given the necessary specialized training to prosecute Internet-related cases. This is actually one of my larger concerns. We are not effectively training prosecutors to go after these crimes. There is a case that is thrown in front of them where we hope maybe the defendant will plead. Many can prosecute aggressively. They are very good at it. They have received the training. But, when you consider the number of prosecutors we have in the State, with all the District Attorneys' Offices, the Attorney General's Office, and the U.S. Attorney's Office, the question is, "How many have ever really received the appropriate training?"

Here is a bigger problem: judges are seldom given the necessary training to recognize the seriousness of this problem. Lenient sentencing occurs far too often under the belief that a real child was not involved, only a picture. The defendant did not actually touch anyone.

The legal dilemma right now is that the Internet and cybercrime technology is a fast evolving area. The government is having a difficult time keeping up with all our laws. It is being challenged in court after court because we are relying on laws that were written years ago, and trying to make them apply to today despite changes in technology.

What we just skipped was a brief video clip from a television cartoon that makes reference to whether the framers of the Constitution and Bill of Rights really knew what to expect back then and how we seek to apply them today. It dealt with an argument over the right to bear arms. One of the characters representing one of the framers turns back to his wall and says, "What do you mean, everyone has the right to hang a pair of bear arms." On the wall is a pair of bear arms. This comic relief raises the question of whether we know what was really intended, and whether the laws we are currently writing will be applicable five years from now when the technology is completely different.

Let's move on to Nevada laws. Nevada has worked to protect children through the passage of various laws. I do not think anyone would argue that Nevada does not want to go after these people.

This slide shows the most of the laws that apply to the sexual exploitation of children when it comes to concerns like online pornography. NRS 200.710 makes it unlawful to use a minor to produce pornography. NRS 200.720 deals with promotion of the sexual performance of a minor. NRS 200.725 deals with preparing, advertising, and distributing materials depicting child pornography; so distributing it is covered. NRS 200.730 deals with possession of visual presentations depicting sexual conduct and possession of child pornography. NRS 200.735 is the exemption for law enforcement, allowing law enforcement to possess child pornography.

Current Nevada Laws

- Nevada has worked to protect children through various laws passed
  - NRS 200.710 Unlawful to use minor in producing pornography or as subject of sexual portrayal in performance.
  - NRS 200.720 Promotion of sexual performance of minor unlawful.
  - NRS 200.725 Preparing, advertising or distributing materials depicting pornography involving minor unlawful; penalty.
  - NRS 200.730 Possession of visual presentation depicting sexual conduct of person under 16 years of age unlawful; penalties.
  - NRS 200.735 Exemption for purposes of law enforcement.
  - NRS 205.486 Unlawful use of encryption.

Additionally, there is a statute, NRS 205.486, that deals with unlawful use of encryption. If they are encrypting child pornography, there is an additional criminal charge for attempting to conceal it.

Very briefly, I would like to discuss some issues with these NRS provisions.

NRS 200.720 deals with promotion of the sexual performance of a minor, and NRS 700.725, preparing, advertising and distributing. Under 720, where the minor "engages, stimulates, or assists others to engage or stimulate" sexual conduct or where the minor is the subject of sexual portrayal, is a category A felony.

However, under the definitions, "promote" means to "produce, direct, procure, manufacturer, sell, give, lend, publish, distribute, exhibit, advertise or possess for the purpose of distribution." This really covers everything under NRS 200.720, "promoting the sexual performance of a minor." This covers distributing it. Right now we have people who are being charged with distribution of child pornography, who did distribute it, which is a lesser crime than this, so it would be a lesser included offense. [NRS 200.725 and NRS 200.730 are category B felonies.] Then we have this charge that is seldom used, and which carries a life sentence, with parole possible after 10 years. Five years, I believe, if the child were 14 or 15 or over. It is a better charge to use.

The problem we have right now is that this statute [NRS 200.700] and we have the distribution statute. The problem is with prosecutors understanding the differences. Why would one apply and the other not apply. I think this is something the Legislature needs to clarify.

"Promoting" means to "produce, direct, procure" and all those things. Would it be any different from someone making magazines available to people who come in his store to view child pornography? They are promoting it. They are making it available. They are saying, in effect, "Come look." They are showing a film, and they allow people to come into the movie theater to watch child pornography. This person is promoting child pornography, because he is distributing it, exhibiting it at that time.

Someone who allows child pornography to be copied from their computer to a file sharing network is promoting child pornography. They are getting it and distributing and exhibiting it. Often, they know they are allowing other people to come get it.

Here is another part. We sometimes get too technical with these crimes. It has come to be expected by the courts, prosecutors, and investigative agencies to make these really technical. Earlier, the Board discussed credit cards and people's private personal information, and credit cards being transmitted from one place to another.

My concern is that a guy who takes my credit card number at a restaurant I go to. After it receives money from Visa or the bank, then someone throws out the receipt in the dumpster outside and someone can just go get my credit card number. Sure, it can be done on line, but you also can go into the back alley and get it quickly.

I say this because there is also a non-technical way of doing things. A crime is a crime. I am trying to encourage people not to get too technical with computer crimes. It is what it is. There is either evidence or there is not evidence. There is a confession or there is not a confession. Either the law was violated or it was not.

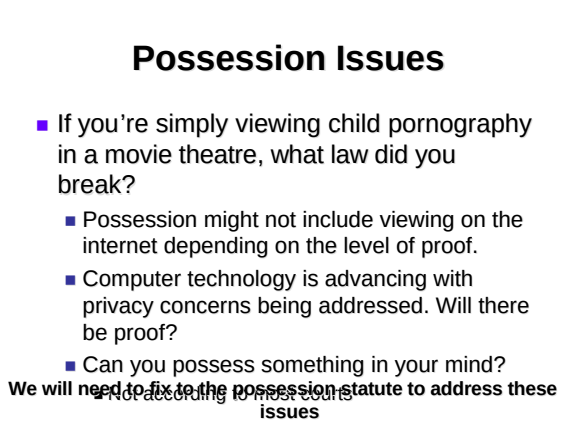
This is the distributing statute [NRS 200.725]. I am not going to discuss it in too much detail. But, let me ask, is this really any different that the promotion statute [NRS 200.720]? Or, should this statute really apply to those who prepare child pornography but do not actually distribute it? You can distribute something or prepare it or advertise it without it ever touching your hands. You can be a corporation in California or another state that allows it to be prepared. You advertise it, you

make arrangements for it to be distributed, but you are not allowing it to be viewed from your computer. There is a difference. I think these two statutes need to be clarified.

This also addresses an important developing issue. What about schools, juveniles, and cell phones? The statutes deals with “a person who knowingly prepares.” It does not say “an adult.” It says “a person.” This is a problem around the country right now. There is a juvenile being prosecuted in Ohio. There are juveniles who have been prosecuted in Florida who took a nude photo of himself and sent it to a boyfriend.

Right now, I have no direction as to whether I go with cases like this. We are getting these calls in schools. We are mandated to investigate child exploitation, which is what this is. A child taking a photograph of himself, and sending it to someone else is child exploitation per the definition. We are going to spend a lot of time and resources investigating cases that maybe should, or should not, be prosecuted. In most cases, there is no criminal intent with these kids just sending a picture to a boyfriend. This is something that really needs to be addressed.

The next important slide deals with possession of child pornography, NRS 200.730. The first offense is a category B felony; the second is a category A felony. Both are punishable by only one year in prison. The second offense is up to life, but an offender could be sentenced to as little as a year.



Possession in the statute deals with actual, physical possession. If you are simply viewing child pornography in a movie theatre, what law have you broken? If you simply attended, but someone else is showing the movie, what law did you break? If you go on line to virtual world, and someone is showing child pornography, and you know that room is going to have child pornography, and your avatar enters that room so that you can watch it streaming down onto your computer screen, your computer may or may not hold that as evidence, depending on the type of program and what your computer settings are, but what law did you break?

“Possession” might not include viewing in the Internet depending on the level of proof. Certainly, I think we could prove that someone intentionally searching for child pornography who enters the appropriate key words, was guilty. We might be able to argue that. But we are relying on what the Nevada Supreme Court, the Circuit Court and, ultimately, what the U.S. Supreme Court will say our statute means.

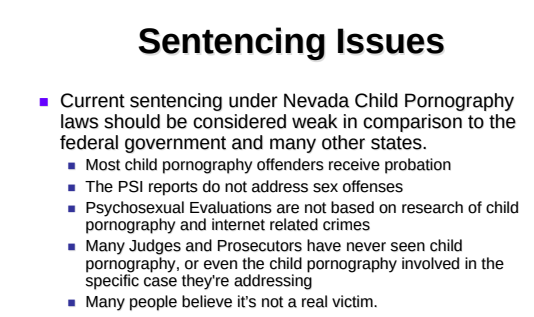
Computer technology is advancing with privacy concerns being addressed. Will there even be proof? Most Internet browsers that are being released today have settings so you will not have a history of where you visited and what you were doing.

The question is, can you possess something in your mind. Most Circuit Courts say, “No.” They say you actually physically have and intentionally go for it. We are going to have to fix the possession statute to address these issues. People who intentionally go to a web site, watch streaming videos, go to a movie theater, or just go into a book store they know carries specific child pornography – We are going to have to fix the statute to make it clear that intentionally viewing child pornography is an offense. I know the concerns that will come up. Those concerns deal with pop-ups and accidental downloads. We can prove that. Most of the time that occurs after someone has already confessed that they are intentionally looking for child pornography. We can prove those cases, but we need to address it.

Just to wrap up, here is a quick NRS conclusion. Will the current laws be OK? The laws we have now, are they OK? Well, probably, maybe, could be, yes maybe no. The answer is, "I don't know." It all depends on what a judge determines down the road, but we have time to fix things. The statutes can be clarified to avoid issues.

Unfortunately, the Legislature meets every two years. We saw that with the Internet luring statute. A problem came up that we could have fixed. That had to do with what specific charge was being applied. A question with a law came up. We had the time in that Legislative session to fix it. A decision was made to fix it at that time, because there had not yet been a Nevada Supreme Court decision. Two years went by, and we could not charge the offense as we would have liked. So, if we get to matters before that, it is even better.

The last thing are sentencing issues. Currently, sentencing under Nevada child pornography laws should be considered weak in comparison to the federal statutes and those of many other states. We are considered weak. We are considered weak by most of the other investigating agencies I work with from other states.



Most of the people we sentence in Nevada to child pornography are receiving probation. Federal government sentencing, the U.S. Attorney's Office, federal judges, all that is different. In Nevada, most people possessing child pornography are receiving probation whether they have one image or 100,000 images.

Right now, the pre-sentencing investigative reports that Parole and Probation prepares for an offender, before sentencing, do not even really address sexual crimes. It is just a general investigative report. It does not address it, and it should be changed. Someone will receive a psycho-sexual evaluations before sentencing in a criminal case like child pornography and these other crimes. If you read them, most of them will say that the standards they are using have nothing to do with child pornography. But yet, that is the crime they are being sentenced for, because there have not been enough studies about child pornography. But, as you will see in the near future, according to some studies, as many as 85% of child pornography collectors have victimized a child whether they have admitted it or not. That is being discovered through post-conviction polygraphs.

Many prosecutors and judges have never seen child pornography or even the child pornography involved in a particular case. They hear "child pornography", the defense stipulates to "child pornography" because they do not want that kid shown. The judge has no idea what it looks like. They might think it is just a 4-year old, or 7-year old, or 10-year old child standing there next to a tree, naked. In fact, it might be a 3 or 4-year old child being brutally raped by an adult male.

Unfortunately, in sentencing, there is no distinction based on what type of videos or images this person possessed.

Also, many people believe there is no real victim. It is just a picture or video. There is no sentencing guideline in Nevada or enhancement for the following: the amount of child pornography the defendant possessed. Again, it doesn't matter whether they have one image or one video or 500 or 500,000. It is the same thing for sentencing.

The level of severity of child pornography is not involved. We see child pornography where, an investigator will say that in their experience, is relatively tame – it might be a child alone in a

sexually explicit position. It is not a child being brutally raped. There is no difference in how the courts are sentencing those people. There are no criteria right now.

Well, where does this take us? Law enforcement must dedicate resources to investigate this. Prosecutors must commit resources to prosecute it. Laws need to be reviewed and updated before it is too late. We really need to get on those. We can not guess where technology will take us, but we need to be prepared. Technology in two years can be completely different. Everything I am talking about today might be completely out of date and no longer apply. We might not even be able to do computer forensics in two years if the right company were to come out with encryption that we just could not break. We do not know what will happen.

Where this takes us

- Law Enforcement must commit the resources
- Prosecutors must commit resources
- Laws need be reviewed and updated before it's too late
- We can't guess where technology will take us and need to be prepared
- Investigators are drowning in cases
- Where will two party consent leave us?

But, investigators are drowning in cases. I can tell you that. We have far too many cases compared to the number of investigators we have.

I do want to mention two party consent, though I will not talk about it very much because of time. Nevada is a two party consent state when it comes to interception of communications. There are a lot of other states that use a one party consent rule, specifically for child exploitation investigations, including child prostitution and on line crimes. They are able to solve many cases we can not solve now. Many of our cases rely solely on a confession. If we do not have a confession, we do not have a case. It is difficult sometimes to get a suspect to confess to what he has done to a child. But, it is very easy for a child to ask a suspect over the phone, "Why did you do this to me?" thereby, getting the suspect to admit something to them. We can not record that conversation in Nevada at present. We can do it if it is a federal case.

I apologize for having to rush through some of this. I would have liked to explain more. I would be glad to come back anytime. Do you have any questions?

AG CORTEZ MASTO:
Detective Carry, thank you very much. I apologize that we did not have more time to go through more of the specifics. You are welcome back anytime. In fact, I think there will be an opportunity for us to work together in the future for some of the issues you have concerns about. Let me open it up to Board members. Are there any questions for Detective Carry? Hearing none, thank you again.

I appreciate the Board members staying over 15 minutes.

Agenda Item 10 – Public Comments. (Non-Action Item)

AG CORTEZ MASTO:
Are there any members of the public in the south who would like to address the Board?

SHERIFF GILLESPIE:
No. There are not, madam Chair.

AG CORTEZ MASTO:
There do not appear to be members of the public here in Carson City who want to address the Board. We will move on to Agenda Item 12, our adjournment.

Agenda Item 12 – Adjournment. (Discussion/Action Item)

AG CORTEZ MASTO:
Thank you very much for being here. We are adjourned.

Meeting adjourned at 12:17 p.m.

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on August 12, 2009.