Minutes of the
Technological Crime Advisory Board

September 5, 2013

The Technological Crime Advisory Board was called to order at 2:00 PM on Thursday, September 5, 2013. Attorney General Catherine Cortez Masto, Chairman, presided in Room 2241 of the Legislative Counsel Bureau, Carson City, Nevada and via videoconference in the Grant Sawyer Building, Las Vegas, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Nevada State Assemblywoman Irene Bustamante Adams (Advisory Board Vice-Chair)
Nevada State Senator Aaron Ford
Professor Hal Berghel, University of Nevada, Las Vegas
Dennis Cobb**,** Co-Director of the UNLV Identity Theft and Financial Fraud Research & Operations Center.
James Owen**,** Deputy Chief, LVMPD, *meeting designee for Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)*
Darin Balaam, Assistant Sherriff, Washoe County Sheriff's Office, *meeting designee for Mike Haley, Washoe County Sheriff's Office*
David Gustafson, State Chief Information Officer, Enterprise IT Services
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Interim Special Agent in Charge Gil Lejarde, *meeting designee for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)*

ADVISORY BOARD MEMBERS ABSENT:

Daniel Bogden, U.S. Attorney, Department of Justice (DOJ)
Tray Abney, Reno/Sparks Chamber of Commerce
Resident Agent in Charge Kyle Burns, Homeland Security Investigations

STAFF MEMBERS PRESENT:

Belinda A. Suwe, Executive Director
Henna Rasul, Deputy Attorney General

OTHERS PRESENT:

Samuel Kern, Deputy Attorney General
Brett Kandt, Special Deputy Attorney General
Lea Tauchen, Retail Association of Nevada
James Elste, Nevada Cyber Initiatives
Craig Schmidt, Microsoft
Jim Wall, Microsoft
Special Agent Jason Berryhill, United States Secret Service

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

AG CORTEZ MASTO:
Good afternoon. The first item on the agenda is a call to order and the verification of the quorum.

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

AG CORTEZ MASTO:
I'd like to recognize Senator Ford who is joining us for the first time. Welcome to this committee and we look forward to working with you and to your input on this important issue for the state. We're happy to have you, thank you.

SENATOR FORD:
Thank you very much. I volunteered to sit on this Board and I am happy to be here.

Agenda Item 2 – Public Comments.

AG CORTEZ MASTO:
This is the time for members of the public to address the Board. There will also be a second opportunity at the end of this agenda. Are there any members of the public here that would like to address the board at this time? Seeing none, we will move on.

Agenda Item 3 - Discussion and Approval of Minutes from June 26, 2013.

AG CORTEZ MASTO:
The next item on the agenda is the approval of minutes from the June 26, 2013 meeting. A copy of the minutes was provided ahead of time. Please take a look at the

minutes, and I'll open it to any discussion or a motion. Is there a motion to approve the minutes?

Motion to approve the minutes was made by Mr. Uffelman and seconded by Assistant Sheriff Balaam.

The motion to approve the minutes was unanimously approved.

Agenda Item 4 – Reports regarding Task Force and Board member agency activities

AG CORTEZ MASTO:
Would any members of the Task Force like to report at this time?

SA JASON BERRYHILL:
Thank you Madam Chair, I am Jason Berryhill, Electronic Crimes Task Force Coordinator with the Secret Service. Fiscal year 2013 is coming to an end for us, but it's been a busy and productive year. As most agencies can attest to, the success of the Electronic Crimes Task Force relies heavily upon our state and local partnerships. I'd like to brag a little here, for those that haven't heard of the National Computer Forensics Institute or NCFI, which is DHS operated, but the program has actually been run by the Secret Service since 2007. The goal of NCFI is to train state and local partners in how to deal with cyber fraud, respond to network intrusions, and conduct computer forensic examinations. Just this year alone the Las Vegas task force was lucky enough to get 8 officers trained: 3 from Las Vegas, 2 from Nevada Attorney General's office, 1 from Reno, 1 from Sparks, 1 from Washoe County Sheriff's Office and in total we have 7 forensic investigative partners. In less than 12 months they've analyzed a total of 334 devices. To break that down that's 30 flash drives, secure digital cards, and smaller items, 148 cell phones and 156 hard drives and that comes out to a grand total of storage value in the amount of 29.58 terabytes. To give you a concept of how much volume that is, a single terabyte can hold 100 copies of the Encyclopedia Britannica and 10 terabytes can hold the entire printed collection of the Library of Congress. So, that's just shy of 3 libraries which is pretty impressive. That's all I have Madam Chair.

AG CORTEZ MASTO:
Jason, thank you, and let me say, on behalf of the staff of my office, thank you for the training that you are sponsoring for us to really obtain a lead on cyber fraud, computer intrusions, and forensics. It's so important not only for our office but for all of law enforcement across the state and we really appreciate the collaboration and

partnership. One final thing, as part of the National Association of Attorneys General, I quite often go to the national meetings and we had the opportunity to receive a presentation from the folks who actually put on the training for NCFI, and it is impressive. Not only the level of training is impressive but the number of people who have been trained at that facility at the local, state, and federal level is also impressive. So, I can't thank you enough and we appreciate you participating with us on this Advisory Board. Would any other task force members like to speak?

ASSISTANT SHERIFF BALAAM
Thank you Madam Chair. As I spoke last time from the ICAC (Internet Crimes Against Children) task force, we've identified those who are becoming our repeat offenders. So, Sgt. Dennis Carrey that's assigned to that unit is working on an action plan of how we can better target those individuals since we're seeing a trend of more and more people that have been convicted numerous times of some type of crime against children and continue to repeat. Sgt. Carrey is working on that in collaboration with Las Vegas Metro and their unit. We continue to work on this as it's a pressing issue.

AG CORTEZ MASTO:
Thank you, and for everybody's benefit, I actually have an investigator that sits on that task force, and I hear from my investigator how busy that particular task force is dealing just with the child pornography that comes across their desk through the internet. It's amazing to me, and I appreciate everything that the task force has accomplished. The task force in the North has been busy continuing with search warrants and forensic exams. We're seeing an increase in investigation requests from agencies as technology becomes more intertwined in our lives and thus becomes of greater importance in criminal investigations. We're seeing a lot more requests from outside agencies requesting assistance in conducting forensic exams.

Agenda Item 5 – Report by Craig Schmidt, Senior Manager, Microsoft Digital Crimes Unit, Discussion on Public/Private Partnerships to Combat Cybercrime.

AG CORTEZ MASTO:
Before we begin, let me say that working at the national level with all of my colleagues, Microsoft has been a fantastic partner of ours and we want to thank you for not only coming here and talking with us but everything you do at the national level to work with at least the state AGs. I know you're working at all levels of government but we really appreciate the collaboration and partnership with the AGs.

JIM WALL:

General Masto, My name is Jim Wall, the director of state government affairs with Microsoft. I just wanted to introduce Craig briefly. As you and many others are aware, we're proud to call Nevada home. We've had a growing presence in Reno. They are very committed individuals who are very active in the community here. As I've come to town and spoken to legislators, you, Craig, and our global team who specialize just on digital crimes, I think there's a lot of collaboration that we can do in addition to the collaboration we are already doing. This is beyond our normal commitment to the state and we thought this forum is an appropriate forum to bring one of our global experts, Craig Schmidt.

CRAIG SCHMIDT**:**
General Masto, thank you having me here. I know that your time is valuable. As I get talking if you need me to stop or restate anything, feel free, this presentation is for your benefit. A little of my background, I've been at Microsoft for 5 years and I've been on the digital crimes unit the entire time. Before I came to Microsoft, I was a federal law enforcement agent doing cyber-criminal investigations with the Air Force OSI. My focus was mostly on counter intelligence and counter espionage, but of course when dealing with cyber type issues, the areas of child protection and human trafficking come up. And, of course, it's a balancing act trying to distribute resources. I know the impact that it has on people's lives is devastating. I've also seen how technology has drastically changed how this fight is being fought. Hopefully I'm here to give you some help and information that you can use to try to protect the public.

I have a brief video that goes through background and history of the where the digital crimes center came from. *Video played*.[1] Summing up everything the video said, obviously the mission of the Digital Crimes Unit is we want to transform the fight against digital crime through leveraging partnerships, legal breakthroughs which are novel in theory, as well as technical breakthroughs. The ultimate goal is we want to disrupt how cyber criminals operate. It's so easy to compromise computers and to social engineer people that the risk is worth taking. There's things that technology companies can do to help play a role in making that barrier a little higher, but we obviously can't do it in a vacuum. We very heavily rely on partnerships. From the legal perspective, one of the things that have been a little more unique is in the majority of botnet takedowns. You'd think you use some kind of cyber law, but we actually use trademark law. There are also civil seizure components that are part of it. So, we took a different approach to it. The attorneys that we have on staff are pretty creative. And, again, not creative in a standpoint of going too far, but the solution isn't always legislation. There's room for you to do things, you just have to think about it a little bit differently. As far as technical

[1] Presentation materials available at http://ag.nv.gov/About/Administration/Tech_Crime_Meetings/

breakthroughs, photo DNA was mentioned in the video and we'll talk about it more in depth, but it's a technology that we license away for free. We've licensed it to places like Facebook and Twitter, and Microsoft obviously uses it. It's a way to preemptively take child pornography off of your services before it gets distributed. We also license it to law enforcement and there's also tools available to use as well that I'll discuss in greater detail later. So, again, I'm sure most of you are aware of what a botnet is, but just in case, I'll hit it from a really high level. A botnet is like an army of infected computers and there's any number of ways that this can happen. It doesn't necessarily have to be through a vulnerability in an operating system. I can remember one example where somebody was advertising a site as Lady Gaga dies in car crash, which is fake, but if you search for Lady Gaga, you may be tempted to click the site. If you go to the site, it will say in order to read the news story you have to install this codec. They have to do that because the operating system is actually secure. If they could silently install the botnet, they wouldn't need the prompt. But, it dupes the user into accepting yes and what they are actually saying is that they are allowing this malware permission to be put on your machine. That's the majority of what happens, so obviously some of it is an educational issue. Once the computers are infected it becomes under the control of what we call a bot herder. Think of it as a mastermind person who can task the computers to do his bidding whenever and wherever he feels fit. Once the machines are infected, the all report back to the bot herder. Once they are reporting in, the bot herder can essentially task them to do any number of things such as stealing credentials or hijacking searches. What hijacking searches means is that if, for example, you go to Google, Bing or Yahoo and type "car insurance." Underground organized crime syndicates will hijack the searches and then sell the leads to the insurance companies which pay money for such insurance leads. So, for example, if I am an affiliate for Geico, Geico will pay me $40 if I get someone to sign up for insurance. So, I would go to a search engine and try and put my site into the keywords so that I can show up, but obviously I will have to compete against Geico. So, how can I outbid Geico to sell Geico back their leads. I could use stolen credit cards or hijack searches. So this malware, what it will do is when the user types in "car insurance" it goes out to the search engine, gets the real results, but it will inject behind it their own site. When the user clicks the link, it doesn't matter what the link is, it will actually take it to a different site. We've had examples where a person searches for "60 Minutes" and wanted to view 60 Minutes episodes. 60 Minutes doesn't charge for their content but if you had this malware installed, you went to a duplicate website that looked exactly like the real 60 Minutes site, but you had to pay to watch the videos. So, you're talking to a criminal and there's no way for you to know this. The criminals can also use this to spy on you. We had one malware that had between 10 and 15 machines infected with it and one of the things it did is it would remotely turn on the microphone and the camera of your computer and it would eavesdrop. So, you obviously wouldn't want this in your

home but you can also imagine if it were in a business or in a federal government agency it could be a really big threat. This is also the source of all your spam and this is also how all the DDOS attacks happen. You've seen in the news recently how banks have been taken offline or Syria launched attacks against newspapers. Those are almost universally through infected consumer computers. They can also be used to spread more malware. So, once the person has a foothold they can in essence side load more threats onto those computers. Through the research that we've done, on average, once a computer has an infection there are 27 other infections. In other words, the infection gets resold over and over to 27 other individuals and they'll all get paid money to put things onto those computers. So, it's a very big problem and difficult to stop. I mentioned this before but the reason this works is because the cost for the bad guy doing business is very small and the value of the infection is very high. Again, there's this lifecycle that an infected machine will go through. We had another threat we'd taken out called Zeus where it would steal banking credentials and would wire all the money out of your banking account. It would spoof the screen so you couldn't tell. It would look like your money was still in your account so you wouldn't report anything to the bank, but then after the money is gone, you would get notices of insufficient funds. Of course when the money is wired it looks like a legitimate wire transfer. The money is gone and the bank isn't really under any responsibility to get the money back. Over the course of 2 years this group from Eastern Europe had stolen over $580 million. Over 80% of the victims were in the U.S. How do you hear about this? Even if you had something like this on your computer, who do you report it to? Even if the end user knew they were infected with Zeus, what are they going to do about it? There's not a lot of information on how to address these issues. One of the goals of our team is to reverse this. We want to increase the cost and lower the value. Again, there's only so much you can do there's a certain group of people that don't really care, the laws are there for the people that don't need them. If they're going to listen to the law we wouldn't have this issue. But, what they will listen to is the value. If they infect a computer but they won't make any money doing it, then the problem will fix itself. So, that's what we're in the process of trying to do. We've had some of these botnet takedowns in the past few years and here's a small sampling. We've worked with a lot of partners in taking down these botnets. Our stance has been that any problem that affects a consumer affects us as a company as well. Microsoft has over 100,000 employees so we are in essence our own consumers and enterprise. Things that impact consumers and enterprises affect us as well. We have tons of consumer services and our employees use our services. We're a diversified enough company that we honestly can't take a one sided approach. So, we have a unique approach of what's good for everybody is good for us. It's really in our interest to have the internet be clean and trustworthy. We have a timelapse video of infected computers checking in with us after we've done a takedown. The number that you're seeing is the number of

machines coming from that geography. So, if you think back to the botnet slide, when we go to the court and get permission to take one of these threats out, we in essence become the bot herder. The machines report into us and we work with SERTS and ISPs to go and clean those machines, but in the mean time they are pointing at us. Again, this is something that we need to broaden the amount of partnerships that we have to try and get these machines cleaned. You would think that especially since we've worked so actively with trying to get these machines fixed that the rate would go down but they get infected at the same rate we are cleaning them. But, we do offer free tools for all this and we work closely with a lot of people to try and get the curb out of this. When we take one of these threats out, that threat in and of itself technically isn't a problem, but like I said earlier, there are on average 27 other infections on these machines so it's these individual's behavior of using the machine's is what's being identified so they're kind of habitually infected. When I was a law enforcement agent, I had a number of investigations that had come up where I was like I need some information from Microsoft and how do I get this? You can get trained, but this world is constantly changing. I didn't find this out until I became an employee of Microsoft, and I was almost mad to find out that Microsoft had a program and was trying to give me assistance. So, our mission is to partner with law enforcement to provide them with tools, training, and technical support. This is for free, we don't charge for any of this. We have a portal online and I have a screenshot of what it looks like. We also offer it in different languages. If you have a crime that occurs in Nevada and there's a nexus to Lithuania and you wish you had a contact in Lithuania that you could work with to get an idea of the size of the problem, on the portal we have a way that you can link up with those people. Everyone sees the portal in their native language, so you can write it in English and they will see it in Russian or whatever dialect they have. It's a pretty effective tool. We also have about fifteen 100 and 200 level training videos for forensics and investigators. We also have hands on support so they can email and ask us specific questions and we'll get someone to answer. We can also help in instances where say you get an image of a machine and you want to use something like live view to try and boot into an environment. If it's in windows it will detect it as being a new computer and it will ask you for product keys, we'll give you product keys for free that you can use during your investigations. Of course it's all vetted so there is an area you can access if you are an academic or an industry partner, but there's a certain area that is just for law enforcement. We do checks to make sure that you're actively law enforcement and that area of the site is completely separate from the rest of it. We're not saying that you have to disclose or discuss investigative information. It's protected and a point to point type. We don't house the information and it's done in a very secure method. We're here to help people get the help that they need. The vision of the site is to bring together all of these different areas under a community so we can work together as industry, law enforcement, and academia. It's called the digital crimes

community.com. Investigators or anyone else that wants access to it just has to email dccphelp@microsoft.com and you'll be walked through the process of how to get access. This is a screenshot of the portal. There is an area again where if you're law enforcement there's a tools section. We have some forensics tools that we provide for free and also the discussion board and whatnot. This also has information on how to get subpoenas to Microsoft or preservation letters, so basically our criminal compliance. Also, you can contact us if you want to get product keys or a specific forensics question such as how to install exchange and you need to verify the source of an email, or really in depth questions. We typically have about a 24 hour turnaround time. I very rarely see it take longer than that, so it's pretty up to date.

Now I'd like to transition to the child exploitation problem. Before the internet was a prevalent utility there were a lot of entry barriers to child pornography. You had to find a victim, take the pictures, get the pictures developed, and you had to know somebody that had the same interests. There were geographic barriers and there were many steps that made it easier to get caught. But the internet has changed that completely. There are no more fences or barriers to this. You can have 1 picture that gets sent billions of places simultaneously and that child gets victimized over and over again. One man can have over a million child porn images on his computer, just outrageous stuff. This is something that realistically is only feasible because the internet and computers exist the way they do. From a technology perspective, we thought we have to try and do something about this. Once these images get taken, the victimization happens over and over again. While I never had to do any child pornography investigations when I was law enforcement, I saw the impact it would have and I met with people who were victims. It's a horrible thing and I can't fathom it. The solution we came up with is we worked with Dartmouth University to come up with a new method called photo DNA. Some of the typical problems you have when you do forensics is we typically rely on hashes. If you think of it as a fingerprint, the fingerprint should be unique and if you found the fingerprint, you found the person who left the mark. Pictures don't quite work that way. If you take a picture and you upload it to a service on Flicker or Twitter those services make minor changes to the image. Even a very small change in the metadata where it's not perceivable in the image itself, it will alter the hash to the point that it will no longer match. Also it creates a problem from scale, the second that an image gets shared if you seize the computer and you find the child pornography, you'd never be able to match it with anything that was shared with anyone else because it's fundamentally changed. So, what photo DNA does is it takes an image and converts into greyscale and then it calculates different intensities within the image and cuts it into smaller blocks. The point of it is that it's able to match images that have been changed based off a fuzzy type hash. So it's not that you can identify the exact person in the image, but it will identify that images are similar enough that it's

beyond statistical anomaly that they are the same. We've licensed with the technology coalition and they're using it to help analyze all the photos that they have coming in. I know that their roll out on it is fairly small. We've done some pilots with them where just for testing purposes they were taking some of the worse of the worse that dealt with infants and other really bad stuff. They've had a lot of success and this is something that we license for free but there are also some third party tools that use this that are also free for law enforcement. The internet is full of all of these images and if we had one that was child pornography or something offensive, how do you distinguish between the floods of images. This is a visual breakdown of how photo DNA approaches this. If the image is flipped, or the exposure is changed, or zoomed in, in a traditional hash, those would be viewed as different images. But with photo DNA it recognizes them as the same image. From a photo DNA perspective it doesn't have the problem with a traditional hash that interprets small changes in the photo as being different photos. So it uses a multitude of parameters to increase the accuracy of identifying the same pictures. Traditionally there was a 1% chance that the same image could be identified, but photo DNA has increased that 26%. So that's a 26 time percent improvement. The tool that we licensed out for this that we authorized is made by a company called Metclean called Analyze. Again, that's a tool that's free for law enforcement. It's a utility that you can feed images to that will generate photo DNA hashes and identify which images should be focused on. There is some configuration you can do if you're worried about false positives. Of course, nothing's always perfect, but it is a huge asset to be able to scale these types of investigations.

Now to talk about sex trafficking. This morphed over time. Originally you had websites like Craigslist or Back Page that had gotten into this seedy underground where it was basically the hookup for linking sex traffickers together and smuggling individuals. Again we asked what we can do to help stop this. We identified a bunch of areas to focus which include the advertisement and selling of victims and the searching for and purchasing of victims by Johns. We're still in the early stages of this. We got some grant money of about $180K that we've gotten together from the company and it's with 6 different researchers right now. This next Monday they are supposed to report back to us to let us know what they've come up with. But this is an area we're focusing on over the next year to see what we can do to help tackle this issue.

From our perspective, our trying to protection our customers is similar to the goal of an Attorney General's perspective of trying to defend your citizens. That's where I think we share the same goal. I think one of the things that we as a company have learned the hard way is that we have to try and think of cybercrimes in new ways. Like the example of using trademark enforcement. It's not just about patching an operating system. There's an education aspect, but there's also a responsibility by us as a technology

company whose services can be leveraged to do this. From a citizenship perspective we have to take an active role in this and we definitely want to do that. We want to work together to make positive change happen. We don't want to be in a vacuum. As a company, we're not in a position where we can succeed by doing that. This also means that we have to share information and foster innovation. That's one of the reasons why the digital crimes unit has morphed a little bit. We're creating a concept of a cyber-division to expand this role with the intent that we want to encourage cooperation between individuals with very specified talents and roles not only within the company but also with industry and government. And, just to be clear, if I identify a Hotmail account with child pornography, I have to go through the same steps as law enforcement. I have to write a subpoena to get a search warrant, etc. through our attorneys. So we treat ourselves the same as law enforcement so we're doing it the right way. We have to take an active role in combatting cybercrimes rather than leaving it to its own. We have a responsibility to do something about this and we spend a large amount on it. It's a very serious commitment on our part. We have an announcement that will likely be coming in October where we officially launch our new cybercrimes center. It's a very significant investment, and it won't be the only one that we have. There will be other satellite sites. This will also be something where the goal of the majority of what we want to accomplish will need the assistance of other people. So, we're actively looking for partnerships and ways to make a positive impact on this area.

DR. BERGHEL:
There's been a particularly effect category of malware called ransomware lately. The one that I have in mind is the FBI money back scam. You didn't mention it, but it seems to be particularly virulent. Can you give some account as to why it's so virulent and what steps you've taken to prevent it?

MR. SCHMIDT:
I am familiar with that. I know that we have some cleaning tools that can address that. As far as why it's as pervasive as it is, there's any number of ways that malware can spread. A lot of it actually comes from advertisements which are a tricky thing to investigate. I have some definite information on how that works, but the business model itself is really complicated. I think the reason why it's pervasive is it's too easy to infect people and to get them to fall victim to scams. We have a report that comes out yearly that goes into the theory of how computers are getting infected and I believe about 60% of infections come from social engineering. So, again it's someone who is unwittingly duped into allowing the installation of software onto their machine. There were campaigns that I've come across that were what we call drive by downloads through malicious advertisements. Again, we do have off line free tools that people can use to clean their machines.

AG CORTEZ MASTO:
What type of outreach do you conduct knowing that when you were law enforcement you were unaware of what tools Microsoft made available to local law enforcement? I suspect our law enforcement in our urban areas are probably in touch with your group already and are working with you, but we have a lot of rural communities and local law enforcement in the rural communities that have limited resources but that deal with these issues quite often. What type of outreach do you do to them, if any, and how can I refer them to get in touch with you or your unit and to understand what resources might be available?

MR. SCHMIDT:
Typically, we partner with Attorney Generals, and depending what the circumstances are, we try to work it with a larger event. In May we did an event with the Attorney General of Massachusetts in which close to 400 people attended. We did training there the entire time. This next year we are going to double our capacity that we have at that event. We also work with NAAG on events. As far as getting individual or one on one relationships, it's more of a grass roots effort. Again, usually working with AGs, but word of mouth and letting them know to contact us and to ask for access to our sites and tools. Unfortunately, I only get so much budget and hopefully that will change. But the AG component is pretty critical.

MR. WALL:
The AG probably has a better relationship with the departments and knows how to contact them, so we would be happy to provide you our contact information and you could, in turn, send our information onto the local law enforcements.

AG CORTEZ MASTO:
This is great and we were just talking about doing some training with our rural law enforcement partners and some of the D.A.s specifically on the sex trafficking component but I think cybercrimes in general. If you guys already have a curriculum or even come out for onsite training, I think that's fantastic. We can organize the meeting and find the site and get law enforcement in the room, but we need the experts to come in and train.

MR. SCHMIDT:
Absolutely. We usually try to make the biggest impact we can. Typically, we don't like charging for this type of thing, and we try to find a way to make it work. On average we try to do between 5 and 10 trainings a year. But if we can get enough people to show up at one place, we could justify it. We usually do something for 2-3 days for 6-8 hours

so it's pretty in-depth. We bring all of the computers and everything. There was talk with NAAG to do one on the west coast to try and get more people rather than focusing on the east coast so much, so we're waiting to see how that works out. The goal for me is to get people the help they need.

AG CORTEZ MASTO:
I appreciate that, thank you. Thank you for coming today, it was definitely eye opening. I know that my office will be reaching out to you to determine how we can work together not only on this but other issues that I know we have in common. Thank you.

Agenda Item 6 – Report by James R. Elste, CISSP, CISM, CGEIT, Chief Cyber Strategist, Nevada Cyber Initiatives, Discussion on Internet Privacy Issues.

AG CORTEZ MASTO:
Jim has been a great friend to this board and has always provided this board with any assistance we've requested. So, I want to thank Jim for being here with us today.

MR. ELSTE:
Thank you, it's good to be here. I really appreciate the opportunity to come and speak to the board today about a question that I don't think gets addressed directly in discussions, which is privacy. Privacy is a very interesting aspect of the cybercrime challenges that we face. It speaks to the heart of some fundamental principles in our country and in our society. What I'm hoping to do today is really frame a discussion around privacy and in some respects set up what I hope will be further discussions in privacy for this board. The place I'd like to start is with defining privacy. I'm sure everyone's heard this phrase because it's the primary retort you hear when you mention privacy which is "if you have nothing to hide, you have nothing to fear." If you don't take anything else away from my discussion today, please don't ever use that phrase again. It is really hard to support in a rational discussion on privacy. As an example, most people that use that phrase, if questioned on their private matters for a period of time usually capitulate and very quickly decide that's not a rational argument. We do need to come up with a definition of privacy that we can use as a working definition that helps us understand the privacy balances that we have to strike. Justice Brandice back in 1890 published what is one of the most important legal papers that has ever been written in regard to the right of privacy. What he said is privacy is the right to be let alone. He suggested it's the most comprehensive of rights and one of the most valued by civilized man. This was in a time before we had cell phones, computers, and all the technology we have today, but it's still a very fundamental principle which is that right to have privacy. What we have to be able to do is define exactly what we mean by privacy, we have to understand how we value privacy and how to assess the value of privacy in a

social setting and then how do we weigh privacy against the countervailing concerns of national security, law enforcement, etc. What I would propose is a definition that's been circulated that's a bit more expansive and bit more precise in terms of what we think about privacy. Privacy is a right to keep a domain around us that includes things like our bodies, our homes, our property, our thoughts, our feelings, and our identity. It's the ability to decide which parts of that domain we're going to allow access and to what extent we're going to allow said access. If you think about this in practice, it's who we choose to make a friend and tell our secrets to or who we invite into our homes. These are fundamental principles of control around those things that matter most to us. With that definition in mind, I want to change the framing of this to help you understand the forces at work that affect where we are with regards to what we think appropriate levels of privacy are. Lawrence Lessing out of Harvard Law School wrote a rather interesting book call Code 2.0 and there are certain sections in it that deal with identity and privacy and he proposes that there are four forces at play: technology, market forces, social norms, and laws, regulations, and policies. Technology, as we all know, evolves very quickly. It's kind of agnostic when it comes to social norms and policies and we wind up with technology that does things we've never thought of before. The second most quickly moving force is the market force which steps in and says wow, that's a really neat piece of technology and we can make money doing this with it. What happens then are social norms start to adapt to that technology and those market forces. So we see changes in what people's expectations are from the social norms perspective. Regrettably, what follows most slowly are the laws, regulations, and policies where we try to instantiate those social norms and regulate the market forces and technologies. With those four forces in mind, there's a lot of tension between them. The market is always going to try and take advantage of the technology to try and minimize regulation. Social norms are going to adapt as technology changes and they're going to try to bring that into the regulatory environment. What I'm going to do is in four sections talk about the four forces and what's happening with regards to privacy.

Technology is really the fascinating part. I've been a technologist my entire career. To take you back to that definition of privacy regarding the physical domain, the communications domain, and a thought domain. I'm going to take you to the most extreme end of the technology spectrum right now and ask you what you'd think about privacy if it came to the thoughts in your head. U.C. Berkley did a study in 1999 where the image on the top is being shown to a cat and the image on the bottom is what the technology is able to interpret from the cat's brain. So, the technology is able to essentially determine that the cat is looking at the image of a face. So the question becomes what does that look like when you use it on humans in 2011. An individual was shown a movie with elephants walking across a field and the technology could determine that there were elephant shapes being rendered in that person's brain. An

individual watching an airplane or a bird flying and the technology could see not a perfect rendering of that plane or bird, but certainly enough of a rendering to determine that person was thinking and cognizing the visual images that they were seeing. When our thoughts are suddenly subject to technology and exposure, privacy becomes even more important. There's another thing that's been happening with technology that I think we sort of sense and know, but haven't really thought too much about, and that's the digital fingerprints that we're leaving as we use technology. We generate tons and tons of information in the transactions that we have online and the types of things that we use technology for such as smart phones and credit cards. All of these technology devices leave digital fingerprints. We leave these fingerprints in our health records, our financial records, we leave them in terms of things we contribute to the government, things that we use our identity for, relationships that we have, and activities that we take part in. All of these leave a technology fingerprint and, in some cases, we're able to actually construct information about an individual that helps you identify the individual and the behaviors that they're engaged in. This is an example of the type of thing that can be produced with a digital fingerprint on an individual. This is the location tracking of an individual with where they went and what time. At 7:30 they went to the coffee shop for coffee, 9:00 am they went to work, 5:30 they went to dinner, 7:00 to church, 10:00 to theater, 11:30 to the bar and 2:00 am they were at the donut shop. You can infer just by knowing that information that this person has a job, goes to church, likes the theater, drinks, and eat donuts at 2 in the morning. So you can start to develop a profile of an individual's behavior just by those digital fingerprints that they're leaving. That's the sort of technology frame we're working in. We're leaving these digital traces all over, they identify a lot of behaviors and information about us, and so the question becomes how do we make sure we're applying privacy in the right places for that technology.

The market forces of course have adapted to this very quickly. Everyone recognizes these companies and these companies have monopolized this technology to do things like build Facebook which is now a huge company that has tons and tons of information about individuals. Google, the search giant, has collected infinite amounts of information about behaviors and what people search for and things that people like when they're searching. Amazon does same thing. The purchasing behavior of individuals is being analyzed so that they can give you better recommendations for products. This is a chart of how EFF, at least one company that looks at privacy issues, rates these different companies with regard to their privacy practices. How strong of an advocate they are for privacy. What you find is a pretty broad spectrum. There are companies that have an eye for privacy and will invest their time and energy in trying to do things like promote privacy rights in congress or fight for their privacy rights in the courts to publish transparency reports and things like that. Others don't really get

involved in that. They don't really spend the time to try and make privacy a part of their organizational DNA. It's not an unfair characterization. The market forces are what they are. They're trying to make money and build businesses that are profitable and so doing things like advocating for privacy or trying to improve privacy aren't necessarily going to be consistent with those market drivers. But there are a lot of interesting benefits that come along with using information in a way that helps the market improve. This is an example from a world economic forum paper which basically shows you two things: improvement in the hospital performance when they didn't publish patient outcome data which was 13% for average hospitals and 7% for low performing hospitals. When you publish the health outcome data and the hospitals were able to improve with that data available to them, the low performing hospitals improved 40% and the high performing hospitals improved 22%. So, there was a significant improvement by having access to the data. What we don't want to do in a privacy argument is decide that absolute privacy is the requirement because there are benefits to be had by having an appropriate disclosure of information and utilizing that information in appropriate manners. That brings us to some of the models that are taking place which are future models of online privacy. We know there are these exchanges of information taking place. One of the models being put forward and is quite compelling is the notion of a personal data store. So you would have certain information that's defined as your personal information that you would have the ability to regulate the transaction of that between the consumers of that information, organizations that are requesting access to personal information about your health records, financial records, etc. and those entities that possess those records or otherwise serve up those pieces of information. So these are the cutting edge models in privacy for helping the individual have an ability to be part of that transaction. To not simply be unaware or uninvolved in an exchange of information that involves their private information.

This is where we start to see the social norms aspect. People are starting to become more aware of the value of their information and the types of things that information is being used for and the consequences of using that information. Daniel Solov is probably one of the leading minds in privacy right now. He's a professor at George Washington University in the Law School. He's written several papers that have become the guiding documents for modern privacy in the technical age. One of them that I'll share with you is why if you have nothing to hide you have nothing to fear is such a bad argument. The others are what he refers to as the taxonomy of privacy. It explains among other things that privacy is in many respects a function of the consequences of sharing the information. This list is some of the consequences or harms that he identifies that help you understand the types of things that could happen with regard to the information about an individual that really reinforce the notion of

having privacy as a fundamental part of our society. We don't want people being subjected to blackmail. We don't want people being embarrassed or otherwise having exposures of data that damage their reputation or we don't want to have information being used in ways that the individual did not originally intend for it to be used. If I provide health information to my doctor to help with a diagnosis I don't want them sending that information over to the insurance company so they can evaluate raising my insurance rates. I don't want them using it for subsequent analysis. What I do want though is if they have a need for that information to be involved in that decision to share my information. I want to be an active participant in having stewardship over my own private information. These harms really do illustrate in a way that's more complete than simply the things we naturally assume for privacy. We all sort of have a visceral response when we think of a surveillance society where you can't do anything or go anywhere without that being recorded or otherwise have no shelter. The Orwellian approach to life. But there are many more harms that go with privacy violations that are worth considering and will reshape the social norms that we are subject to because people are aware of how technology is being used and becoming more savvy users. The benefits of privacy in many respects are legitimate benefits that people want to see supported. So we see things like the consumer privacy bill of rights being published by the White House which identifies certain constructs for privacy that help shape how people use information and help them determine whether they are or aren't using it in a way that's appropriate for privacy. So you have things like individual control, transparency in the way that information is being used, respect for the context of that information, how people are applying security to that information, and whether that information is accurate which is a really important part. We collect a lot of data and that data is not always right. That the information that's being collected is limited by what's needed, it's not just being collected wholesale and a certain amount of accountability for these companies and organizations to the consumer with regard to their information. There's another thing that the FTC put out with the department of Commerce and there have been several iterations of this, but this is the Fair Information Practices Principles and this is the beginnings of the foundation of establishing good practices and it's similar to the Consumer Privacy Bill of Rights. The two are documents that have been essentially constructed with the same frame which is people are entitled to notice, consent, participate, transparency, security etc. One thing I would like to draw your attention to is the enforcement and redress section which says that the FTC identified 3 types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil cause of action for individuals whose information has been misused; and then government enforcement which can include civil and criminal penalties leveled by the government. So what they envision from an enforcement perspective is having everyone involved including the individual, the organization and the government.

This takes us really to the last part of this which is what do we do from a legal and regulatory perspective. It's surprising when you think what sort of privacy laws are there? Nevada has 603A which is our breach disclosure law. But there's actually quite a few laws at the federal level that have been written which establish certain elements of privacy around things like communications, financial transaction, government collection of information, and medical records (HIPA). The interesting thing about these laws when you look at them is that the latest of these laws was written in 2003, over a decade ago. As we talked about at the beginning of this discussion, technology changes very quickly so in 2003 Facebook didn't exist, we didn't have social media the way it exists today and all of the things come out of that that leave you questioning what is the social norm now for doing things like sharing pictures of yourself in rather compromising positions. It's fascinating to see how the younger generation adapts to the technology and what sort of social norms they apply. Privacy is also in many respects about shaping the behaviors of people with regards to what should be considered private behavior or information. When you look at things like COPA and one thing I do hate about coming to the tech crime advisory board meetings is all this child pornography and child sex trafficking stuff is distressing. But there's an element of this that's relevant from a privacy perspective which is you have to start by protecting the private information and privacy of the children making sure that things like COPA are being enforced so that we don't have children inadvertently or otherwise going to sites that they shouldn't be going to or otherwise exposing them to danger. A lot of the privacy regulations are designed to protect us and the information that we should be considering quite valuable. I think it's a fascinating part of the frame we're in from a technology perspective. I think there's a variety of really compelling issues when you think of it from a technology, market forces, social norms, and regulatory perspective. I hope this is the first of many privacy discussions for the Tech Crime Advisory Board. I'd be happy to answer any questions.

MR. GUSTAFSON:
Jim, you really hit on something. Because of the Snowden issue and all this stuff about Prism coming out now many people looked at this and thought well, we kind of figured they were doing something crazy anyway so it didn't really bother us. Others were shocked and awed and running for cover. But I think the value of that is now we're actually talking about what is privacy and where that boundary is. I think as a society, it's good that the leaks came out. I kind of suspected the NSA would be doing this stuff, but what's important is the meter. Where on the gauge or the meter is the line between privacy and protection. Because right now there isn't a clearly defined line between what is private and what is not. Kids go on Facebook and share everything, including naked pictures. The older generation, including myself, I don't do those things

purposefully because I don't want to share that kind of information. Where is the society line at for how much information you share and what is private and what is not. I think it's great that we're having this conversation now and I think it's going to be relevant. It goes back to the guys at Microsoft. A crime is breaking the law, but what's acceptable and what is not is what determines what the law actually says. And so we need to talk about where that line in privacy is drawn and I'm glad we're starting the conversation on this. Thank you.

MR. ELSTE:
Thank you David, and you've raised one of the fundamental challenges in privacy. We often think of this as a security vs. privacy discussion and it's really not. Matter of fact, when I was a security officer in Health and Human Services, I would go to the chief privacy officer and ask him that he tell me what needed to be protected and I would tell him how. We tend to think of privacy and things like the NSA matter in the context of a tradeoff of either or. And really I think we need to understand that this is a multi-faceted problem. You certainly don't want to be operating at any of the extremes. You don't want to be an extreme totalitarian environment where there is no such thing as privacy and you cannot forgo the national security and law enforcement interests so that you can have absolute privacy. So, it is about understanding it well enough that you can strike a balance. A lot of the current thinking in this is about what is referred to as contextual integrity. In the context of certain situations, it's appropriate to have violations of fundamental privacy considerations such as exigent circumstances in law enforcement where there is a sufficient probable cause to issue a search warrant you already have the power to negate certain privacy protections that are either in the constitution or in the law. But, the thing that's disturbing about the NSA disclosures is that the common wisdom has been that the NSA has some very sophisticated techniques for electronic eavesdropping. That's their mandate. We've always known that they've been developing those techniques. The individuals such as William Benny who have come out and said this is really much worse than you think, they're doing all these things, came out and said that but never brought anything that represented some sort of evidence on it. And what Snowden has now done is said they're doing all these things and here's a slide deck that proves what they're doing and we have evidence now that supports the conclusion that they are using those powers and capabilities in ways that might be of concern for many privacy and civil liberties perspectives. The New York ACLU filed a law suit several weeks ago against the NSA basically claiming that the NSA interception violated Attorney/Client privilege and the privacy rights of members of the ACLU in New York and within their national organization. The brief for that was rather compelling. They're communicating with clients who are bringing forward concerns about civil liberties and trying to engage in litigation and those emails would be attorney/client privileged communications. In my opinion, it's not a matter of

right, wrong, or otherwise with what the NSA is doing and I think we can all reasonably believe that the disclosure that Snowden engaged in is not an appropriate disclosure. I think we're going to find ourselves as a country and as a global community, because there's a lot of countries that aren't really happy that their president's and members of parliament etc. have had their stuff eavesdropped on, in a dialogue about what is appropriate for intercepting or otherwise gaining access to electronic and digital communications. I think once again it reinforces the importance of discussing privacy in a venue like this because somewhere down the road there's going to be legislation that comes out that we're going to have to take and come to grips with. How will it impact law enforcement? How will it impact the state of Nevada and how the state of Nevada positions itself with regard to privacy? The good news in my opinion is we're going to have the debate. The bad news is the means that got us to the debate. It's really quite fascinating and I think it's going to be one of those topics that defines us as a generation. We are the technology generation. The folks before us had telephones and they sent letters. We use cell phones and smart phones and email and we have this powerful technology and it is absolutely and fundamentally changing our world. It's going to be what defines us as a generation.

AG CORTEZ MASTO:
Is there any state that has taken the lead in trying to define privacy boundaries and passed legislation to address privacy issues?

MR. ELSTE:
The good news is that Nevada has. Back in 2009 when Nevada passed the encryption statute for 603A, which is our breach disclosure law, we essentially crossed the rubric on it if you will. We said that if you are moving personally identifiable information and you have that in transit, it must be encrypted to a reasonable standard. The state has been recognized in literature as the first to do that, which is fascinating to me. We do have the opportunity as a state to have some leadership is the arena. I think the other state that has done well in terms of security and privacy legislation is Massachusetts, although their approach has been rather fundamentally different. The approach that Nevada has taken has been to provide an incentive approach as there is a safe harbor provision in the 2009 statute which incentivizes business to conform to this requirement. Massachusetts has taken a prescriptive approach that said though shalt have a security program with all these elements and then the sanctions associated with not conforming. This is a target rich environment for legislation. Privacy is something that affects everyone. Every citizen of the state has an interest in their privacy and I think there are opportunities to set some novel legislation. I can give you one example from an international venue. Germany has a law called the TMG that basically talks about establishing anonymity in transactions. One part of the law specifically prohibits an

organization from compiling information that would otherwise de-anonymize an anonymous or pseudonymous identity. It prohibits companies from combining information to determine an identity. If you look at Europe as a whole, they have a very different privacy perspective. You can't ship private information across national borders and they have very broad definitions of privacy and private information. So once again I think there's an opportunity to look at the spectrum of laws that exist and try to figure out where that balance is so that we as a state can produce legislation that is reasonable and balanced and takes into consideration the security aspects and the privacy aspects.

AG CORTEZ MASTO:
I appreciate your comments and absolutely recognize Nevada's leadership and I appreciate you saying that because there are some new members here. But, also, it has been a challenge because we are trying to find the balance between privacy and security and also not hindering innovation. It has been a working relationship with partners along the way to try and figure out what it should look like. It's an important discussion to have because we need to continue down that path. There is no bright line, there is no answer, and there is no model policy out there. I'm not aware that the federal government has even come up with their policy on this issue so it is going to be left to the states and we in Nevada have led that discussion and I think we need to continue to have that discussion while bringing our partners in to figure out the appropriate balance. There's so much information out there. I talk to kids already about their digital footprint and what they're leaving for others to see as they grow up. It's an issue and I also appreciate the conversation, so thank you very much.

DR. BERGHEL:
I agree with what has been said, I'd like to emphasis that the state and federal government will adapt to whatever technologies they have before them. And so there's going to be some changes to the statutes that deal with these sensitive issues of privacy. The question really isn't whether these changes are going to take place but whether we want to be proactive or reactive. I think Jim spoke eloquently as to what happens or what can happen if you're not proactive. I'd remind everyone that this FISA court that's been in the news so much lately was actually an outgrowth of the church committee which I'm sure there are several people on this board that weren't even alive when that happened. The FISA court was created in response to some abuses but they didn't quite get it right so they keep revising it every 10 years and that's exactly the wrong way to do it. Because then you end up with a situation like we have with Snowden and Chelsea Manning where we are trying to figure out how to get the toothpaste back in the tube. It would have been much smarter if we had gotten the appropriate technologists and legal experts involved in the 70s and looked forward a little rather than wait until 2013 and look backwards. I agree with you. This is the time

for us to take a position on this and bring privacy into the active discussion of these and other related committees.

Agenda Item 7 – Discussion and Formation of Internet Privacy Subcommittee

AG CORTEZ MASTO: I believe this is Professor Berghel's recommendation and he and Belinda have been working on this.

MS. SUWE
Thank you Madam Chair. At our last meeting, Dr. Berghel proposed the idea of having a subcommittee that would focus specifically on these technical privacy issues. I've distributed a Memo to provide a starting point for generating a discussion for an internet privacy subcommittee.[2] Dr. Berghel is responsible for a majority of the content of the Memo, so I will turn the floor over to Dr. Berghel.

DR. BERGHEL:
Thank you Madam Chair. I think Jim did such an excellent job in laying out the exposition of privacy concerns that we don't need to talk about the background and overview. So, let me jump forward to the purpose of the board. It is my current thought that we could draw upon some of the indigenous expertise in Nevada to bring people that have active programs going in some aspect of privacy whether that be in litigation, an NGO, as an attorney for a state agency, or individuals that are actively conducting research in privacy. We could bring those people together to have a purposeful discussion of how privacy affects the citizens of Nevada and how we could make recommendations concerning statutes that might be proposed and regulate privacy in the service of the state. So the definition of privacy is offered here. It's not substantially different from the topics that Jim covered. The mission statement I think says it all. The purpose of the board is to focus on relevant privacy issues, privacy crime, and protection of personally identifiable information in Nevada. The board will make recommendations to the Nevada Attorney General and Technological Crime Advisory Board, monitor changes in international, federal, and state policy and legislation regarding privacy protections and serve as an advisory function to the Attorney General and the Nevada Technological Crime Advisory Board regarding the protection of personal privacy in Nevada including, but not limited to, medical data, financial information, location information, and communications. That would be the vision of what we're trying to do and that would be the guiding theme of this subcommittee.

[2] The memo including the changes discussed herein can be found at http://ag.nv.gov/About/Administration/Tech_Crime_Meetings/

MR. UFFELMAN:
It struck me as having a privacy board advise a board is complicated and maybe we should be more creative about the name of this. The other piece is the meeting schedule. If this board is supposed to act on something, I believe it has to be agendized. So to have the advisory board meet immediately prior, there literally is no time to get things done. The quickest you could act on something is 3 months after this advisory group advises that we should be doing something. So, just trying to figure out the logistics of doing it without saying it should meet a month prior to this group which that means a greater time commitment to the extent that there's overlap of membership. I think the idea is good, but these small changes might make it a better operation.

MR. COBB:
I think those comments were excellent and I'd like to suggest as an alternative that it might work better to meet immediately following the TCAB meetings but submit a report ahead of time to get the agenda discussed in this advisory board. The follow up would be then to work on what you need the 3 months before the next report. So you could actually produce something and have it in front of this board, get feedback, and immediately digest it following this meeting and prepare whatever tasks need to be worked on.

MR. UFFELMAN:
I just wasn't sure if we wanted 3 month lag time whether it's forward or backward.

MR. BERGHEL:
I agree with the two previous comments, but right now we're working on a 30 year lag time, so 3 months is a lot better off than we are.

AG CORTEZ MASTO:
Correct me if I'm wrong, the way I see this is it's a subcommittee of this group, so it will have a mission as you have identified here, but it technically is a subcommittee. We have various subcommittees of many commissions that report back to the commission after their work. The other thing I understand from this subcommittee is it's not made up of all the members of this particular advisory board. There's a recommendation that at least 2 members of this advisory board sit on the subcommittee, but the subcommittee would be made up of members outside the commission.

MS. SUWE
Yes, that is correct, we had envisioned members of the community who focus on privacy like, for example, Mr. Jim Elste. People are really immersed in this topic and can provide us with the best feedback. This subcommittee can also act as a filter so

that we can filter out what issues are most important to present to this board. I know not everyone on this board has the time or ability to grasp these issues, so it's a way to take these issues to people who have expertise in this area, so that they can filter and digest these issues and then present it to the board in a way that's more palatable so that board can then move forward with it.

AG CORTEZ MASTO:
Yes, and I like that idea particularly with the topic of privacy. The question I have for everyone if we go that route is are we comfortable with the mission statement and the three areas that the subcommittee would be focusing on. I'm comfortable with it, but I want to make sure everyone else is as well. Is anyone uncomfortable, disagree with the mission statement, or think it's too broad? We know it's a subcommittee and its mission is pretty specific which is fantastic. So, the next question is the timing and how helpful we think that their work would be to us and when they would get it to the advisory board and then the board make up.

MS. SUWE:
The time of the meeting can always be adjusted. It just seemed reasonable to piggy back it to this board because it's a new subcommittee and to make sure that the subcommittee is working with and advising this board. If the majority thinks we should do the subcommittee meetings a month or so prior to the advisory board meetings, that's fine, but as the subcommittee gets started it seems ideal to do it either before or after our TCAB meetings.

AG CORTEZ MASTO:
Who from the Board now would be interested in sitting on this subcommittee?

MR. COBB:
If we can go back to the mission statement, should we narrow it to say something about regarding privacy protections as they relate to technology? Privacy protection as an overall topic involves your house and all kinds of things. Does it need to say information privacy or something more specific?

AG CORTEZ MASTO:
Yes, I think that's a good suggestion.

MR. COBB:
I would like to volunteer for the subcommittee.

AG CORTEZ MASTO:
Dr. Berghel, are you also interested?

DR. BERGHEL:
Yes, Madam Chair.

AG CORTEZ MASTO:
I would suggest that because it's new and because we are talking about what we're trying to create and the direction that we want to go that at least one of our board members serves as the chair of the subcommittee. Just to kick it off and make sure it's meeting regularly, following open meeting laws, and staying on mission with respect to our goals here.

MS. SUWE:
I agree. This is Dr. Berghel's idea, so I imagine him being the chair at least to begin with.

AG CORTEZ:
So, Hal and Dennis and if anyone else is interested, please let us know. Right now, we need to at least vote to create the subcommittee. Is that correct Henna?

MS. RASUL:
Yes, that is correct.

AG CORTEZ MASTO:
At this time with respect to the subcommittee, I'd entertain a motion to create the technical privacy subcommittee of the technological crime advisory board. This particular subcommittee is going to be focused to provide relevant advisement on privacy issues, privacy crime, and the protection of personally identifiable information in Nevada. Their mission will be to (1) make recommendations to the Nevada Attorney General and Technological Crime Advisory Board (2) to monitor changes in international, federal, and state policy and legislation regarding technical privacy protections and (3) serve an advisory function to the Nevada Attorney General and Technological Crime Advisory Board regarding the protection of personal privacy as it relates to technology in Nevada including, but not limited to, medical data, financial information, location information, and communication.

Motion to create the technical privacy subcommittee to the technological crime advisory board was made by Mr. Uffelson and seconded by Dennis Cobb.

The motion to create the technical privacy subcommittee to the technological crime advisory board was unanimously approved.

AG CORTEZ MASTO:
Great, Henna, is there anything else we need to vote on?

MS. RASUL:
No, Attorney General. The selection of members for the subcommittee is an administrative task that can be accomplished by the executive director.

AG CORTEZ MASTO:
Let's give a time frame in which to identify those interested in serving as members.

MS. SUWE:
Hal and I had discussed people we know that would be good members of the board. I hadn't thought of a way to reach out to members of the public.

SENATOR FORD:
I would like some time to think of a constituent that I may want to suggest as a subcommittee member.

AG CORTEZ MASTO:
That's a great idea, and Assemblywoman, you would have the opportunity to identify someone you would like to sit on the subcommittee as well. If you do have someone in mind, please let the executive director know.

MS. SUWE:
The minutes will be posted within 30 days. Interested members of the public can contact me at bsuwe@ag.nv.gov by November 5, 2012 indicating their interest in sitting on the subcommittee. Additionally Senator Ford and Assemblywoman Bustamonte Adams please get me your recommendations as well. If we do not receive enough interest, Hal and I can work together to fill in the remaining spots.

AG CORTEZ MASTO:
We'll also open it up to the board for any suggestions of board members.

MR. UFFELMAN:
The ACLU will likely have an interest in this subcommittee and have someone that they would like to suggest. At the same time we don't want to make it seem that the privacy board is so private that we designate everyone on the board.

MR. BERGHEL:
I would like to add that when we post the notice, we need to mention that we are looking for people that have expertise in privacy issues, privacy litigation, and privacy advocacy. For the subcommittee to be maximally effective, we need to draw upon skill sets that have to do with privacy.

MS. SUWE:
If any of you have other recommendations, like the ACLU, that you would like to reach out to, please let me know, and I am happy to do that.

AG CORTEZ MASTO:
Great, Belinda, Hal, Dennis and I will work together on this to try and at least get the committee members established before our next meeting of the Technological Crime Advisory Board and hopefully have the first meeting of the subcommittee.

MS. SUWE:
Yes madam chair. I think it would be appropriate for us to create a list of members and present it to the board at the next meeting so that the board knows of the subcommittee makeup before the subcommittee's first meeting. The subcommittee could then meet immediately following the technological crime advisory board meeting.

AG. CORTEZ MASTO:
Ok, I think that's a great idea.

Agenda Item 8 – Resignation of Belinda Suwe, Executive Director

MS. SUWE:
I have accepted a position as a Deputy Attorney General with the Nevada Department of Environmental Protection. I thank you for the opportunity I've had to work with each of you in this position. It has been a pleasure.

AG Cortez Masto:
Thank you, Belinda. I know that we had a difficult time filling this position, but I have some thoughts for how we will proceed with filling this position and we will have an emergency telephonic meeting in the near future with that as the agenda item.

Agenda Item 9 – Schedule Future Meetings and Agenda Items.

MS. SUWE:
Thank you Madam Chair. Because of conflicts on December 5, the next board meeting will be held December 12, 2013. In the interim, we will be holding an emergency teleconferenced meeting in order to discuss the appointment of a new executive director of the board.

Agenda Item 10 – Board Comments

None

Agenda Item 11 – Public Comment

None

Agenda Item 12 – Adjournment

AG Cortez Masto moved for adjournment. The Motion was seconded and carried unanimously. The meeting was adjourned at 3:52 PM.

Respectfully Submitted,

Belinda A. Suwe
Executive Director