Minutes of the
Technological Crime Advisory Board

June 26, 2013

The Technological Crime Advisory Board was called to order at 2:02 PM on Wednesday, June 26, 2013. Attorney General Catherine Cortez Masto, Chairman, presided in Room 4401 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in the Main Courtroom of the Attorney General's Office, Carson City, 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
Tray Abney, Reno/Sparks Chamber of Commerce
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
Assistant Special Agent in Charge Gil Lejarde, *meeting designee for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)*
Resident Agent in Charge Kyle Burns, Homeland Security Investigations

ADVISORY BOARD MEMBERS ABSENT:

Daniel Bogden, U.S. Attorney, Department of Justice (DOJ)

STAFF MEMBERS PRESENT:

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

OTHERS PRESENT:

Todd Pardini, Nevada Department of Motor Vehicles
Tod Colegrove, University of Nevada, Reno
Vanessa Spinazola, ACLU
Lea Tauchen, Retail Association of Nevada
Denise Quin
Carolyn Schrader

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.

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 March 19, 2013.

AG CORTEZ MASTO:
The next item on the agenda is the approval of minutes from the March 19, 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. Gustafson and seconded by Mr. Abney.

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?

ASST. SHERRIFF BALAAM:
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 doing forensic exams.

At our last meeting we had in March, I noted the individual that the taskforce had just arrested out of Fernley who wanted to hire a 7 year old and a babysitter. He was sentenced to 35 years in prison and then lifetime parole.

ASAIC LEJARDE:
Gil Lejarde representing the US Secret Service on behalf of SAIC Rick Shields. The Secret Service Electronic Crimes Task Force will be sending the following task force members to the Forensic Institute in Hoover, Alabama for training.

1) Investigator Chris Defonseka, NVAG, Mobile Device Examiner
2) Investigator Todd Bishop, NVAG, Advance Mobile Device Investigator
3) Detective Zach Johnson, LVMPD, Basic Computer Evidence Recovery Training
4) Detective Paul Ehlers, LVMPD, Advanced Forensics Training
5) Detective Tim Miniot, LVMPD, Network Intrusion Response Program

In addition, we will be having our Summer Task Force Partner meeting on August 1, 2013 at InNevation Center (Switch). Invitations will be sent out next week.

AG CORTEZ MASTO:
That's great, thank you.

Agenda Item 5 – Report by Belinda Suwe, Executive Director, Update on Cyber Bills that went before the 2013 Nevada Legislature.

BELINDA SUWE:
Thank you Madam Chair. I wanted to provide an update on the outcomes of the tech crime legislation that Jim Elste presented to our board at our last board meeting. AB 42 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB42.pdf, which was the bill to create a Cyber Institute within the Nevada System of Higher Education, died in committee. The committee felt that the bill wasn't ready as it didn't have a specific curriculum or defined degrees. Alternatively, the committee wasn't sure if they had authority to move forward with this bill.

AB 181 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB181.pdf which prevents employers from demanding social networking usernames and passwords was enacted into law.

AB 385 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB385.pdf which attempted to establish relationships between law enforcement and data depositors died in committee. There wasn't any public support for the bill. The data depositors are currently unregulated and hesitant to support data depositor legislation, even though this legislation was primarily intended to support them. Also, the bill draft that was given to LCB and presented at our last meeting was substantially different than the bill drafted by LCB which may have led to confusion and the lack of public support.

Finally, SB 25 http://www.leg.state.nv.us/Session/77th2013/Bills/SB/SB25.pdf was enacted as legislation. This bill gives the Attorney General express authority to investigate and prosecute technological crimes. This bill also makes some minor changes to our board. Specifically, it changes the voting requirements for electing my position, the executive director, from 2/3 to a majority. Thank you Madam Chair.

AG. CORTEZ MASTO:
Thank you, Belinda. Does anyone else have any other comments about legislation that they are aware of that would affect the Technological Crime Advisory Board? None, ok thank you.

Agenda Item 6 – Report by Samuel R. Kern, Senior Deputy Attorney General, announcements from National Association of Attorney General's Privacy in the Digital Age and National Cyber Crime conferences.

AG CORTEZ MASTO:
Before Sam begins, along with SB 25, it was important for my office to start investigating and prosecuting technological crimes and issues to be prepared for the

future. Our law enforcement on a local and federal level and particularly in rural communities are challenged with resources. We have fantastic law enforcement such as in Carson, Washoe County, Clark County, and the larger urban areas that perform a lot of this work, but the rural communities are challenged merely because a lack of resources. The thought was to bring technological crime expertise into my office and build on this expertise with a prosecuting investigator so we can continue to work on these types of crimes at a statewide level, to assist federal investigations, and to assist the rural communications on technological crimes. Sam is the prosecutor focusing on technological crimes. He, along with Belinda given her legal background and presence on this board, can create a synergy between this board and our rural, state, and federal agencies on these issues. So, you will often see Sam here at our meetings as well as reporting on what he's been working on to this board.

SAM KERN:
Thank you. First I'd like to report on the National Association of Attorney General's Privacy in the Digital Age Conference. There was a general consensus that there needs to be some method to notify individuals as to which information is being collected on them and how it's being used. There were some people who didn't believe that any information should be collectable while others believe there are situations where collecting information is appropriate. One issue that kept coming up was to require some kind of public identification or easily identifiable notification for people to see what information is being collected on them and then allowing that individual to make the choice whether the information collected was appropriate or not. Additionally, if there was a publicly stated policy, there'd be an opportunity for state enforcement under deceptive trade practices or criminal acts. So, it was thought that one solution may be a combination of consumer awareness/identification and a state enforcement component.

Other ideas that were discussed include an opt out provision and children's online presence protection and how those apply to children up to 13 and the protections to those children from inappropriate online pages and whether those protections should be extended to older age groups. One thing I was surprised to hear was that consumer education is the least effective ways to ensure that people are protecting their privacy. There's too much information and the message is lost on the consumer and people aren't able to act on the information. A question that was brought up at the conference included is anonymous data collection really meaningful protection? It seems to be more and more feasible to compile that information and to identify individuals based on that supposedly anonymous information they're collecting. I was also interested in whether there were any solutions that were readily apparent for Nevada that could be easily implemented. One of the things that came to mind while I was there is our

current protections for personal identification does not include the last 4 digits of the social security number. The first 5 digits of your SSN are a readily apparent, there's ways of determining them. So, maybe we should think about whether the last 4 digits of the SSN is something that should be included in that information. Additional topics discussed at the conference included the types of data collection and are some types of data more obtrusive than others. You can opt out of cookies, but at a lot of websites you're unable to opt out, so is that a type of intrusion online or violation of privacy? Another interesting discussion is there have been several reports about different price points being offered based on things such as location, how far away a user is from a store, etc. It ends up in a situation where people in different income groups are being offered different prices for the same goods. There's another study of different prices being based on the type of computer, such as those using a mac computer were offered goods at a higher price. It's something the public should be made aware of.

The National Cyber Crime conference was more focused on developing practical skills for fighting technological crime. One session focused on prosecutors and forensic software and simulation. One interesting aspect was a discussion on Microsoft's efforts to combat child pornography and sex trafficking. They've developed technology to identify these images online and to combat the ways that people hide these images on the internet. Another topic discussed was the Electronic Communication and Privacy Act. While various methods were discussed for collecting evidence from the cloud, the best practice is to get a warrant. So, there may be some ways that we can improve our search warrant statutes to facilitate these data requests. It was a great experience, and I'm happy to answer any questions.

AG CORTEZ MASTO:
The Attorney's General National Committee has regular meetings, sometimes on a specific issue like this one, and the concerns that their offices are having on particular issues. The conferences focused on cyber safety and privacy in the digital age are issues that not only we and this board are concerned with, but all of the AG's offices. One of the primary concerns that I have is how a substantial amount of legal activity is occurring and being facilitated by the internet. For example, illegal or controlled substances are being sold over the internet and how can we manage and stop the illegal activity. Intellectual property theft that is also occurring over the internet. I'm told, and we're looking at this now, the sale of minors into prostitution is also occurring over the internet and how do we address it. How do we get the service providers to work with us to identify these websites and to remove this activity from the websites to stop this activity? One of the areas we are focusing on is Google. A lot of the websites that engage in illegal activity have advertisements on their websites so Google is making

money off of these illegal websites. Quite often the advertisers may not know that their advertisements are on a site where illegal activity is happening. My colleague in Mississippi, who chairs our subcommittee on this issue, actually has investigators going online and purchasing some of these illegal goods so that they can then be referred for federal prosecution. For example, his office is purchasing laced bath salts, controlled substances, prescription drugs and those types of things. We, as a group, are very concerned with this are trying to pull the service providers in to discuss this issue and to work together. We're having some success but also some failures. We're still struggling with this issue, but it gives you an idea of where the AGs are and how we talk and cooperate on a regular basis to address a lot of these issues.

DR. BERGHEL:
First, with regard to tracking software cookies, I've written an article on the topic coming out in September. One of the things we've found is that since the practices are unregulated there's an awful lot of abuse, some real and some imagined. There is a feature on our browsers called "do not track me." It's not part of the standard configuration, but if you wish, on a server you can opt for a "do not track me" option. In 2011, Microsoft set up the do not track function as the default in internet explorer 11. So, in response, servers were set up to reject those browsers. Secondly, one of the things that came out of the discussions that arose from the NSA security breach is some of the SCOTUS decisions regarding the 4th amendment reflect that there is no 4th amendment protections of information provided to 3rd parties. I didn't know that. Building records, libraries, telephone records, etc. are not protected by the 4th amendment. So, the question is, what kind of protections do the states offer their citizens to afford them some insulation from the data collecting means of organizations? Thirdly, I have a suggestion. Several members of the public in Nevada have gained some expertise in digital privacy. What kind of interest would there be in the State of Nevada, as maybe a subcommittee of this group, for people who represent the state in issues of privacy and developing for example, white papers and a report on the privacy issues in Nevada.

AG CORTEZ MASTO:
I think you are absolutely right that 4th amendment protections don't necessarily apply to private individuals or companies, but rather only when there's government involvement. That's why recently there are reports coming out about data protection and how much the private sector is collecting data on individuals for advertisements and catering advertisements to the individual based on their profile. The private sector collects all of the data without any concerns of running afoul of the constitution, but the government cannot. I think a lot of people do not realize that, and maybe they want it that way.

Government can only access the data through warrants and complying with certain protections that are in place, but private sector and corporations can and do gather all of this data, particularly to sell and advertise to you based on your profile. I do not think the general public either recognizes this or they don't care. I'd defer to our legislators, but I think a state can legislate those privacy protections within the private sector to protect the public. I don't think there's anything stopping that. It's just a matter of bringing it before the legislature, having the public hearings, and focusing on the law. And to your third suggestion, I think a white paper is a fantastic idea. Gathering the privacy information for our state would initiate a discussion on what would and wouldn't be beneficial. Just having that discussion, putting it in a white paper, and then delivering it to our legislators and bringing awareness to the people that are in a position to pass state laws to address those needs is of benefit. At the same time, we've got a great board. We've got Mr. Abney who represents the chamber in Northern Nevada. We want to respect what those corporations use this data for. That's why we need to have an open conversation with everyone in the community about this issue. I think it's a great idea.

MR. COBB:
Madam Chair, listening to this conversation gave me a thought. Regarding the data collected, no one evaluates the discriminatory purposes. For example if a fundamental aspect of life, say in the 2020s, is going to require online access to sites, the site could potentially deny you access unless you give the ISP full access to your data. There's a discriminatory effect to privacy. Another thing I was thinking about is I recently encountered a PDF service agreement for software that was 17 pages long. I'm not capable of understanding it, especially since I don't have a legal degree. I would like to see either at the legislative level or the commerce environment a requirement of greater transparency. For example, instead of a single "I accept" button for a 17 page document, they could make it so I had to accept different clauses therein related to more or less intrusive aspects of what they're going to do with the information collected on me. I kind of agree with the idea that privacy is not necessarily an issue of voluntariness or education. But at least for somebody that was interested in it, if it made me stop and click several boxes to surrender full access to my data, it might have some effect.

AG CORTEZ MASTO:
It's the new frontier and there are no controls. And, that's the struggle. How do we put the protections that are necessary in place and how do we make people aware? The information that people put on the internet and make available to the public without realizing it is just amazing to me. They're giving all that data away. But, alternatively,

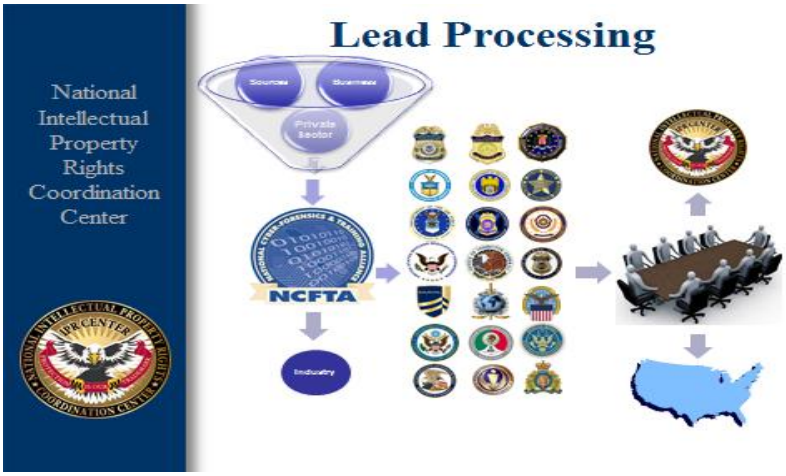
some companies are legitimately using this data to offer services to their customers. For example, at Zappos customer service is key for them. They collect data on their customers for an important reason. So we need to find an appropriate balance between the two.

DR. BERGHEL:
Well, Nevada has a history of paving the way in this area, for example with our encryption bill which includes safe harbor provisions. So, I think there's some wiggle room where if we focus on safe harbors rather than penalties, it may be able to pass, and we could create some legislation to help protect privacy.

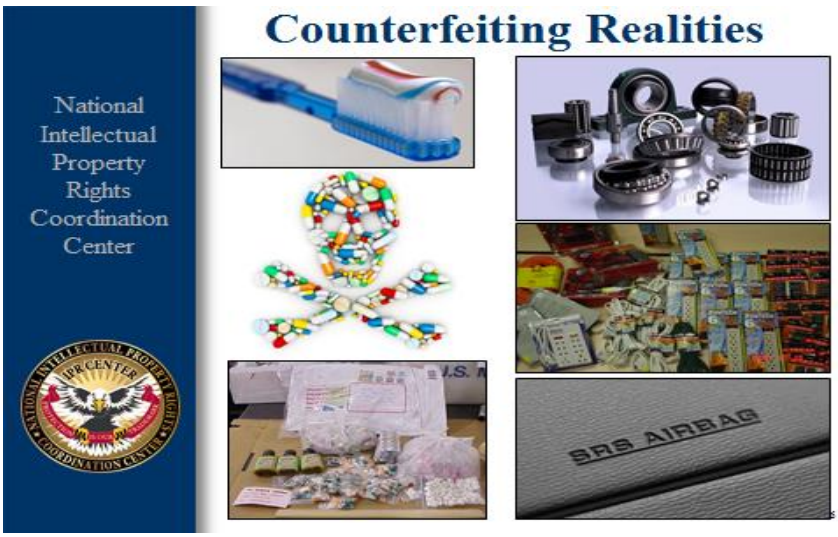
AG CORTEZ MASTO:
These are great ideas and conversation.

Agenda Item 7 - Report by Kyle D. Burns, Resident Agent in Charge, Homeland Security Investigations, Discussion on Homeland Security's actions to prevent websites that infringe intellectual property rights.

RAC SHIELDS:
Madam Attorney General, distinguished members of the board, thank you for allowing me a few minutes to discuss Homeland Security's efforts to combat intellectual property theft. Before I start, I'd like to give a few minutes background to explain why Homeland Security is involved in counterfeit websites. After the attacks on the United States on 9/11 the government had the biggest reorganization since the 1940s. They took 22 separate agencies and combined them to form Homeland Security. The two primary agencies under Homeland Security that are charged with enforcing border crimes are Immigration and Customs Enforcement and Consulates and Boarder Protection. The best way to think about this is boarder protection is the police department and ICE/Homeland Security Investigations is the detectives. In 2008, Homeland Security started the National Intellectual Property Rights Coordination Center in Crystal City, Virginia. This was at the urging of congress. Congress wanted one voice moving ahead and attacking this crime that they realized was not just a threat to money coming into the United States but public safety as well. Currently the IPR Center is led by Homeland Security Investigations as we currently hold the system director position. FBI and possibly border protection hold deputy director positions. There are 21 federal and international agencies that encompass the IPR center: 17 of which are domestic and 4 that are international. INTERPOL, Europol, SAT, which is the Mexican Tax Authority, and Royal Canadian Mounted Police.



This slide[1] describes the lead process and how we get information from the public or individuals and filter it to law enforcement. We take information from all over the place: businesses, confidential informants and sources, other law enforcement etc. That information is sent to the national cyber forensic training alliance. We have HSI agents that are stationed there and they take all of that raw data and they create an intelligence report that is then funneled to all of the agencies you see there in the middle. They have a weekly deconfliction meeting and at that point they decide whether this information should be pursued with enforcement and the agency that has the most to gain jurisdiction wise will take that. Alternatively, it can be refered back to industry for civil remedies. When we think of counterfeiting, most people think of fake Gucci, fake jerseys, fake super bowl merchandise. Those are legitimate threats to people's livelihoods and companies lose hundreds of millions of dollars a year on counterfeit goods. But, the biggest threat that we see is that to public health and safety. Examples include counterfeit pharmaceuticals, phony microchips, and counterfeit airbags. We've done testing on toothpaste that's contained chemicals that are harmful in nature. We have medicine that people are taking that they think will help them, such as anti-cancer medicines that in reality have no medicinal value. In fact, these medicines may actually include chemicals that can be harmful. We've had electric strips and power sources that catch on fire as soon as they are plugged in. These injuries are not anecdotal, but rather these are actual factual instances of individuals being hurt by counterfeit items. For

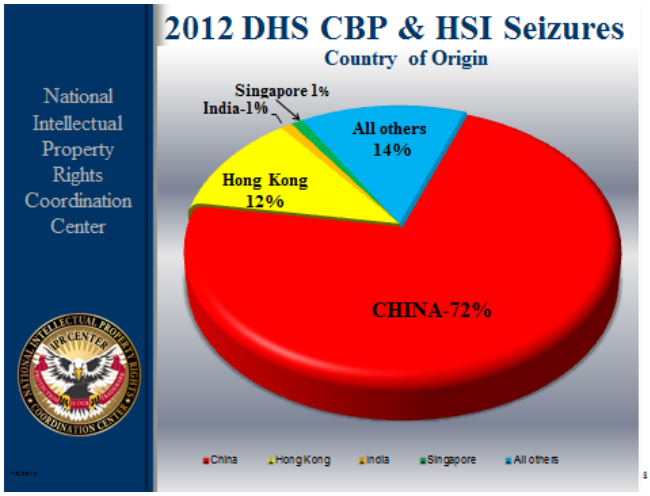


[1] Not all of the slides presented to the Board are incorporated in these minutes.

example, we have videos[2] illustrating the difference between counterfeit and legitimate airbags where the counterfeit airbag may explode in a passenger's face rather than helping to save their life.

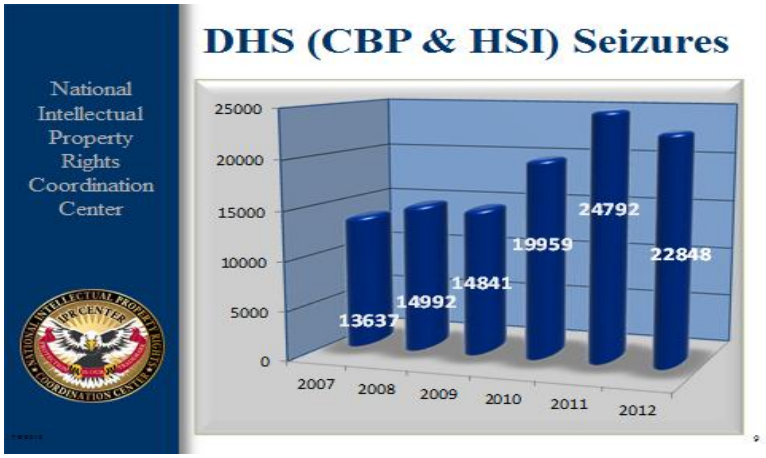
AG CORTEZ MASTO:
How are counterfeit airbags being purchased? Online?

SAC SHIELDS:
Yes, typically online. Sometimes the purchasers are companies that don't realize they are buying counterfeits, and I have some slides shortly that illustrate how sophisticated these websites are. Some are individuals that are making purchases online trying to get a good deal.

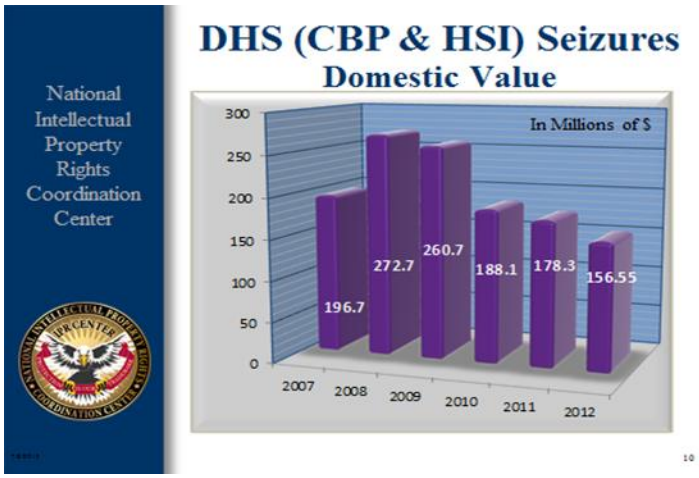


Here is the 2012 chart of where all the seizures are coming from. As can be seen, the great majority come from China and Hong Kong with up to 84%. India and Singapore each account for about 1 percent and then all others remaining. We've had fake pharmaceuticals, for example, from Israel. So, we basically know the source of these counterfeit goods.

This is a chart showing the number of seizures we've had from 2011 to 2012. In 2012, we had 22,848 seizures which comes out to roughly 62 seizures every day of the year. Those are direct seizures from customs and boarder protection or HSI if there is something we may have provided information. The number is going down a little this year. We're not sure why, but hopefully that trend will continue.



[2] Videos illustrating counterfeit airbag failure were shown.



This chart illustrates the monetary value of those seizures. Last year alone, 156.55 million dollars is the estimated value of the merchandise that was seized. The majority of these goods are getting in through express mail such as Fed Ex, DHL, UPS or even regular US mail. Surprisingly, a much smaller amount enters through cargo, but the lion's share is through express or regular mail. We get calls often in Reno of seizures made in San Francisco of fake jerseys, fake pharmaceuticals or fake steroids that are going residents in Nevada. Operation In Our Sites was the HSI's answer to try and combat fraudulent websites. We have a three tier system in responding to fraudulent websites. Most cases will be a tier 3 which includes initiating a criminal investigation and seizing the domain name. Tier 2 includes initiating a criminal investigation, seizing the domain name, and seizing assets, and finally Tier 1 includes a criminal investigation, arrest indictment/conviction, seizure of assets, and seizure of domain name. Since we started Operation In Our Sites we have seized 2075 websites, 1624 domains forfeited, 7 total indictments, 15 total arrests, and 8 total conviction. We've gotten over 118 billion hits to our banner which replaces a seized website. Fraudulent websites may be visual indistinguishable from a legitimate website. It's nearly impossible to tell which website is the legitimate and which is the fake. If I make a purchase from the fake website, in the worst case scenario, Is I get injured by the product and I have no recourse. There's literally nothing the consumer can do. Project Bitter Pill is a subset of In Our Sites which specifically targeted counterfeit pharmaceuticals. We found the registrars of these companies are overseas, Canada and other countries, but the registries were in the United States. Project Bitter Pill commenced in October of 2012 and from that we've seize 686 domain names all from the same affiliate network. The registrar was using a U.S. based payment processor, so the U.S. Government was actually able to seize money associated with these counterfeit pharmaceuticals. For example, lipitorwithoutprisciption.net was selling Lipitor to consumers without a prescription. Consumers had no knowledge of the composition of these pills, and the pills, in fact, had no medicinal value. In some cases, these pharmaceuticals can contain harmful chemicals. So, consumers try to obtain pharmaceuticals cheaply or without a prescription and unknowingly endanger their lives. When we seize a website, it's just like any other federal seizure. A magistrate signs a

seizure warrant, and we put this banner up. If someone goes to liptorwithoutaprescription.net and we've seized it, they will be directed to this website which states the website has been seized under the authority of the United States Government. After coming to the web banner, a user is redirected to a public service announcement showing the dangers of purchasing counterfeit goods. In our investigations, we've linked terrorism to fake DVDs and drugs. A lot of the companies selling counterfeit goods are like criminal organizations. Instead of smuggling drugs, they'll put their money into something like fake pharmaceuticals since there's much less chance they'll be caught. Counterfeits are also associated with child labor and gang violence. As previously mentioned, since we've been putting up these banners with Operation In Our Sites, there have been 118 million hits to these banners, so that's how many people are attempting to access fake websites, whether knowing it's real or not. There have been about 400,000 views of the corresponding public service announcement.

Our Trade Enforcement focuses on public health and safety. That's our number one priority. The public health and safety division focuses on imported merchandise other than pharmaceuticals such as textiles that aren't fire retardant or up to U.S. standards. We're also here to protect U.S. Business and Industry. Hundreds of millions of dollars are being lost by companies that are evading duties or are committing some kind of customs fraud. We recently prosecuted a company that had been abducting Chinese honey. CDP several years ago instituted a massive duty against Chinese honey because they were dumping it into the United States. As a result, some of these Chinese companies are mislabeling or rerouting their honey through a different country. We arrested 7 people and found that they evaded 118 million dollars in custom duties on honey alone. We have textile enforcement teams that travel the world and make sure that there isn't forced child labor and that the textiles themselves are up to snuff and they won't be harmful to consumers in the U.S. We also have in-bond diversion warehouses at customs that hold products that were never meant to be introduced to the US economy. Unfortunately, we also have bad guys that try to steal from in-bond warehouses. They'll say products are being diverted out of the country but instead they will go to the commerce of the US. Again, the government may be losing money and also these are also products that we do not want in the US. Environmental crimes can include cars that are imported from other countries that are not up to code with US

standards. There's a case right now where we are working with the EPA investigating cars that are not up to standards and they found 10s of millions of dollars of fines for that company. We also work to help prevent forced prison and child labor. Finally, we work to prevent tobacco smuggling. We work hand in hand with the ATF when it comes to this, but my agency's jurisdiction is if it touches the border and we will take the lead of anything that crosses in or out of the United States.

Our collaboration between HSI and CBP is basically that customs and border protection acts as the police and we act as the detectives. CBP is going to see things between the ports of entry and they will turn it over to us. It's then our job as special agents to investigate it. We can handle it in a two prong effect: CBP can go after a company as civil fines and we can go after them criminally. CBP currently has a center for expertise and excellence which is a virtual website that importers can use and register and to navigate their way through the process of legally importing goods. Information sharing between CBP and HSI is paramount. Intellectual property enforcement is truly a public/private sector partnership. Without them, we can't do anything, and without us, it would be really tough for them to enforce their rights.

Our office also includes outreach and training efforts. Normally someone from DC would give this presentation, but because of the sequestration and budget issues, I'm giving this presentation. We have what's called the Global Outreach and Training Unit. They literally travel the globe and train the private sector and other law enforcement. We work with the International Anticounterfeiting Coalition, the Attorney Generals, and National White Collar Crime. We are the subject matter experts and we train them and hopefully they train others to help combat what is a massive epidemic in the United States. The IPR Center also provides operational support to the field. If we have a lead in our office, such as a fake item coming in, we're not to try and figure things out for ourselves. They'll either send someone from DC or they will give us direct operational support so we can get what we need to seize those items and hopefully bring charges against the perpetrator. Information sharing is of upmost importance and everyone is sharing information and working together to try and combat these IPR thefts. We've also worked with the Motion Picture Association of America. If you rent or stream videos, the first thing you see now is a combined FBI and Homeland Security Investigation antipiracy warning because we are the primary agency when it comes to enforcing copyright infringement and IPR theft. So, instead of the old FBI banner that used to be shown on videos, now there is the combined FBI and HSI banner before watching a video. The IPR center has also worked with the Motion Picture Industry to have a banner run that states piracy is not a victimless crime and gives the website for reporting IPR crimes seen on most rentals. There's also a report IP theft button on 46 embassy and consulate websites around the United States as well as 12 industry

websites. This is important because HSI is truly a global agency, we have 72 offices in 48 countries, so anywhere that there is a crime we have someone there to respond. When the button is depressed, the user can report IP theft that will be directed to law enforcement. The IPR center is the shining standard for agency cooperation in DC and it's an amazing facility. Are there any questions?

AG CORTEZ MASTO:
Agent Burns, thank you very much. Very informative. I didn't realize the extent to which your agency was investigating and pursuing intellectual property theft. In fact, I'd like to follow up with you after this meeting to talk in greater detail. Thank you very much, that was a fantastic presentation and we really appreciate all of the work you are doing.

SAC SHIELDS:
With an agency like ours, sadly, we've been pigeonholed in the public's mind. Most people think we only do immigration. Our agency is responsible for immigration, but as an agency as a whole we're responsible to enforce 400 federal statutes. The majority of which have nothing to do with immigration, but rather, include drug smuggling, human trafficking, customs fraud, etc. Immigration is important, but our agency has an entire breadth of investigative expertise that we have for things like IPR crimes and we have the support from DC, so if anyone ever has any leads or questions I will be more than happy to speak with you individually. Or, if you need a presentation, I'd be more than happy to do that as well.

AG CORTEZ MASTO:
Quick follow up question: To what extent do the search engines work with you to take down some of these illegal websites? Are they providing cooperation?

SAC SHIELDS:
It works with search and seizure notices. I don't know if the search engines are actively looking for illegal websites. But, I know that if we serve them with a seizure notice or maybe if they get an industry complaint they will shut down the website. The problem is as soon as you shut down one illegal website, another appears. It's a cyclical epidemic. But, to my knowledge there's never been a search engine that has refused to work with us. They seem to want to work with us. Our agency also enforces child exploitation with Assistant Sherriff Balaam and ICAC and I know Google is attempting to eliminate these websites that include this illegal content. That would be fantastic if they could roll that into IPR crimes, and maybe someday they will. But, to the best of my knowledge, they are very cooperative with us and we've been hugely successful in these types of cases. Thank you Attorney General.

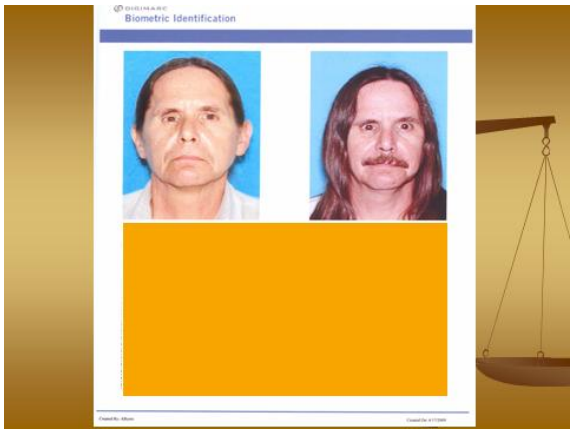
Agenda Item 8 – Report by Todd Pardini, Sergeant, Nevada Department of Motor Vehicles, Discussion on DMV facial recognition software and utilization.

AG CORTEZ MASTO:
I had the opportunity to meet with Sgt. Pardini and his staff to understand these facial recognition capabilities that we had at the DMV. It's really incredible what they are doing and the capabilities of partnering with other law enforcement agencies. So, I wanted to bring this to the board's attention and give you a sense of what the DMV is capable of doing with their facial recognition software.

SGT PARDINI:
Thank you Madam Chair and the board members. Rather than jump right into the facial recognition software, I'd like to take a few minutes to give a brief history of how this came about in the state of Nevada. For those of you that have been in Nevada for as many years as I have, you'll remember the old laminated driver's licenses with the actual photo affixed to it under the laminate. Those driver's licenses could have been copied by a 5 year old and offered zero security features. Then, as well as the rest of the nation, Nevada did not turn a blind eye to 9/11. In fact, the terrorists on those planes were carrying fake identity documents including fake driver's licenses and ID cards from the states. So, in 2002, Nevada went to a digital photo format with the printers on the counters at the DMV, and that is when Nevada started to retain photos. California has been retaining photos forever, but Nevada just started in 2002. With the digital photos and the printers at the counters in the DMVs we were able to incorporate some more security features, but it still wasn't up to standard, and the IDs could still be counterfeited. With the new technologies, Nevada decided to go one step further and get into the central issuance where you don't get your driver's license, ID cards, or permit over the counter but rather it comes to you in the mail. There were many reasons for that move including financial and security issues. The current Nevada driver's license, the one that we issue today has over 30 security features. Some are open to the public, some are only open to law enforcement, and some are only open to the department's investigations unit. There is one security feature that is only known by the director of the DMV and one that is only known by the vendor. When we first starting issuing these IDs in the new style, the thinner ones with the laser perforations in 2006, at that point Nevada had the most secure identity documents of any state. Along with a central issuance we had the opportunity to do facial recognition. If you don't use central issuance, you can't benefit from the facial recognition software. You can't use the facial recognition software on something you are going to print out, hand to someone, and allow them to walk off. Just going to central issuance eliminated a lot of

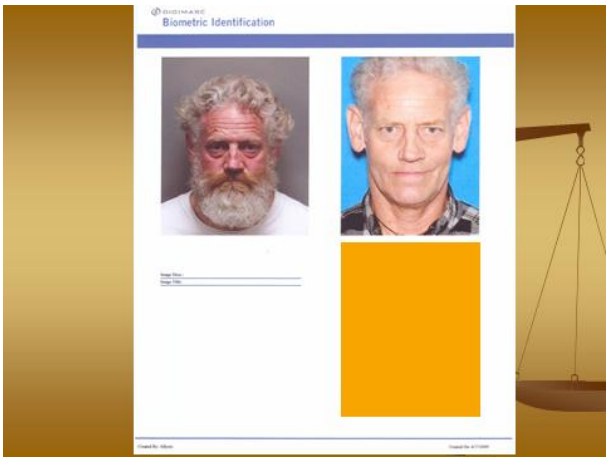
fraud within the department. When we first started the system, we decided to spend the extra money with the vendor, a company called Vigiline, which has since changed hands, and we did what was called a scrub of all the images from the last four years. When we did that scrub list and compared all the photos we came up with a list of about 400,000 possible frauds. It sounds like a lot, but without having facial recognition in 2002, a lot of the photos were enrolled in the system that shouldn't have been. For example, they let you wear glasses, cover half your face, or wear hats, etc. Of those 400,000, they weren't all fraud, but it required my division to go through every single one. With the facial recognition system, before the department spent the money, which was not cheap for the central issuance center and the facial recognition system, the vendor would not disclose the state that it happened in, but they did have a client in the Midwest that found 1 individual with over 300 different identities. That's 300 social security checks, disability checks, etc. Facial recognition is a process of comparing images to determine if they are the same individual. The system is web based with associated hardware. So, when you get your picture taken at the DMV, it creates a mathematical template of the person's face. The computer checks for matches using the algorithm, not the actual picture, because it runs much faster. The system can check a series of numbers and delete the first 10 numbers if they don't match and sequentially go down the line. So, once you get your picture taken at the local DMV it has to be a straight on face, with ears exposed, no glasses or hats. A little PR issue we had was they said you couldn't smile, but yes you can smile. Once the template passes the computer's standards and the computer decides it is an enrollable photo, the photo is compared to all of the other images in the system over two different stages. At the immediate point the picture is taken, the picture is compared within seconds to the last photo on file for that record. So, we can stop fraud right then if we have investigators in the office that this is taking place and we can respond if we are available and take care of the issue at that time. If it does make it through and there is no problem with the enrollment of the photo and comparisons to previous photos on that file, then that night that photo will be checked against every other photo in the Nevada system. There's over 4 million images right now. It's comparing this algorithm, so it does not take into account race, sex, etc. When we first started really getting heavy into these comparisons, we averaged about 18 identity fraud cases per month and about 3.5 arrests, after the facial recognition that went up to 33 identity fraud cases per month and 10.8 arrests. So, obviously, the facial recognition had a major impact on the division. So, if we do have a match overnight we have a personnel in the South that looks at the

matches to determine if they are old frauds, if the photos have been voided. It does hit on identical twins on a regular basis. So, not every match that we receive is going to be a fraud. If the personnel in the south decides that a match needs to be further



investigated it goes up to supervisor in the north or the south and then it's assigned to an investigator. This is an example one subject that was a subject of a facial recognition match. Obviously it does not take into consideration facial hair, length of hair, etc. In one you can see his ears, in the other you can't. The program will not match at 100%. This individual, who was arrested, had been using both identities for 28 years. He collected disability benefits under both identities for 17 years and collected in excess of 180 thousand dollars from the fake identity. He wondered through a cemetery in Reno and saw a headstone of a small child that

drowned in the Truckee River in 1960. He applied for a birth certificate and social security in the dead child's name and was able to commit this fraud. He's currently in Federal prison. This is another subject, and a little more obvious match. He'd been using the fake ID for four years. He came to Nevada about a month prior to a warrant being issued for a parole violation in California so he was just going to live the rest of his life in Nevada under a fake identity. He was arrested and went to the Nevada prison and then back to California. We can upload images provided by law enforcement into the system as long as it's a good photo. I don't know if anyone is aware, but banks are beginning to move their cameras from the ceiling down to eye level which helps dramatically because the better the photo, the better the match, the better the odds. Because the software compares pupils and points on the face, if the photo is blurry or if it's too far away, the match won't be reliable. This isn't a perfect science; this is not walking papers or probable cause to



arrest anyone. This is just another avenue towards the next step in an investigation. As long is the image is a JPEG we can upload anything from a video. Local law enforcement gave us this photo. I believe it is a Washoe County booking photo. He was suspected of being booked under a fake name. When we uploaded the photo into our system we came back with a match. Seventeen years ago he had created a fake identity and proceeded to use two identities. He stole the identity from a man that lived down the street from him in Colorado. We found the victim living in Brooklyn who had experienced no harm, no credit problems or anything. To this day, I still don't know why this gentleman stole his identity but he was convicted at trial in Washoe County. As a division, we are now able to open old cases. In the past, when you got your license or ID over the counter, once you left the building it was difficult to identify you if you used fake information. Once in a while, a criminal will use their real address and we'll just find them but usually they'll use a fake address. We used to have a big insurgence of gangs from Sacramento going to Reno or gangs from LA going to Las Vegas, getting a fake ID over the counter, and then writing bad checks all over town and then heading back to California, but the incentive is diminished since we now use the facial recognition software and the central issuance. The facial recognition software has just about completely eliminated minors coming into DMV to get a fake ID. We've cited and arrested so many of them that the word got out and the minors don't chance it anymore. It's been 2 years since we've had a minor attempting to get a fake ID. Some reasons for identity theft include financial gain, bad credit, they are wanted in another jurisdiction, we don't know why, they have a horrible driving history, drug testing, immigration status, age for tobacco, alcohol, or gambling, or their friend lost their license and they tried to get them a new one. We had a woman who was disallowed from visiting the prisons, so she wanted a fake ID so she could continue to visit her husband in prison. We had another woman who couldn't retrieve her husband's body because she had no ID documents so her sister came into get the documents. And our favorite, we actually arrested a girl because she thought her twin was prettier and she wanted her twin's photo on her driver's license. We do provide assistance for law enforcement. We get calls from law enforcement all over the country. Once we confirm the legitimacy of the law enforcement agency and that it's an active criminal case, we will provide assistance to them. We cannot and do not have the man power to do large requests. Those requests are referred to our records division. We have assisted a lot of law enforcement and a lot of cases have been solved because of this system. One example is Sparks police department had an unwitnessed murder, but they did find a digital camera with individual's photos on it. They gave the camera to us and within 7 seconds I was able to identify the individuals on the camera. Any questions?

DEPUTY CHIEF OWENS:

Would it be possible for a division like mine to tap this facial recognition resource directly? Since you don't have a bunch of people sitting around with nothing else to do to run these inquiries for us, isn't there a way that we could have access the database and software directly so that we could perform the search ourselves without having to tie up your people?

SGT. PARDINI:
That has been talked about, and we have had cursory meetings. I know the Attorney General's office has been involved in possibly giving access to the fusion centers. Whether the DMV is going to open up its records to any law enforcement, I don't know. That's not a decision I would make. But I know as time goes on, this technology continues to change. My agency was the first outside of California to get full access to their DOJ photos and their jail system photos. But, we were accepted as the only agency outside of California as a trial basis. They want to make sure we don't abuse it, etc. I expect this to be an ever expanding technology. More and more states are getting this system. I know Arizona is now looking at it. But when I talked to the law enforcement agent at Arizona DOT, the first thing I told him is they have to get rid of their 30 year driver's licenses. You can't have a driver's license that's good for 30 years and expect this system to work. So obviously that's a big hurdle to jump over. Back to your question, I don't see any reason why it couldn't happen, it just hasn't happened yet and apparently the directors at the right agencies haven't worked it out. It shouldn't be an issue with IT as it's all internet based, but to answer your question, I don't know.

DEPUTY CHIEF OWENS:
To follow up, do you happen to know if any states have banded together such as where you might search Nevada, but it also searches California and Arizona at the same time?

SGT. PARDINI:
Nevada is not linked with any other state. As far as any other states being linked, I don't know. There are several states in the Midwest and East, 16 states have it. Instead of being a real time search, it's rather how we do it where they send you a photo and each state runs their system. California was really close to getting this online before the economy tanked. So, California is going to be busy with it for the foreseeable future if they ever get it going.

DEPUTY CHIEF OWENS:
Thank you, we've had good luck with working with you in the past and we appreciate your help.

DR. BERGHEL:
Do you have any statistics on the degree of collisions you have in your database of templates. For example, where two templates are distinguished by a very small percentage.

SGT PARDINI:
We can set the search threshold that it will not return any results below a certain percentage.

DR. BERGHEL:
Have you looked at all of the templates to see if there are any that are exactly the same that don't match photo identities?

MR. COBB:
Is it possible that the machine produces the same template, but when looking at the photos, the photos are not identical?

SGT PARDINI:
No, I have never seen that happen. We've had this system for 7 years, and I've yet to see a mistake.

MR. COBB:
Is it correct that you perform this through the internet?

SGT PARDINI:
It's all done directly through the vendor and the DMV.

MR. GUSTAFSON:
They just passed a law that you don't have to get your license renewed as often. What result will that have on the system? And secondly, what is the status of RealID?

SGT PARDINI:
They did pass legislation extending the NV driver's license to 8 years. This cripples the system by 50% as far as facial recognition because now you don't have to get a photo as often. It's not something that I was involved in, I'm sure there were reasons for it such as to decrease lines, customer service and all those factors. But, in terms of facial recognition, it does weaken our system by cutting down from requiring photos every 8 years to an even longer span. I don't yet know how the department is going to deal with the legislation. At face value, you only have to get a new photo every 16 years. So, if

that's the case, that's going deplete the long term infrastructure of our system. Regarding RealID, NV was one of the first states to take hold of it and that's what started it. RealID is in its development phase. There's a lot of opposition from a lot of states. So, it's not dead, but it's drastically been pulled back. Nevada decided that if any criminal activity was going to be conducted, whether it be identity theft or acts of terrorism, Nevada was going to its best to make sure it wasn't Nevada identity documents that was used to do it. So, Nevada stepped up, before any of the other states really, and started getting this going and a task force in place and consultations and really took it to task early on. A lot of the stuff we'd already done had to be pulled back because of RealID. So, it'd be up to the federal level now to see what happens.

AG CORTEZ MASTO:
Thank you very much for the presentation and everything you do at DMV.

Agenda Item 9 - Report by Tod Colegrove, Ph.D., MSLIS, Head of DeLaMare Science & Engineering Library University of Nevada, Discussion on advances in 3-D printing and potential criminal activity utilizing such technology.

DR. COLEGROVE:
Madam Chair and esteemed members of the board. As background, I have a Ph.D. in physics and I've been in the high tech private industry for at least 15 years including a number of industries that you've been talking about today including internet service provisions, web posting provisions and so on. More recently, I've gotten a degree in library and information science with a specialty in competitive intelligence and emerging technologies, in particular, to help the guide the direction of where we're going in the library. So, when discussing 3-D printing itself, is this the miracle drug that we've been waiting for? Is this the revitalization of private industry? Or is this sort of the antichrist when it comes to intellectual property and copyright. First, I'll provide a quick background on 3-D printing and the use of that phraseology. 3-D printing has been around as a technology since the late 80s. When you hear the phrase 3-D printing today, what you're really talking about fuse deposition modeling. If you've ever frosted a cupcake with frosting bag where you cut the end off the bag and drew lines in something that was soft and pliable, you're using fuse deposition modeling, except in most cases today we're dealing with ABS plastic or PLA plastic. ABS plastic becomes soft and squishy at a temperature around 200 degrees on up to 500 degrees Fahrenheit. PLA, rather than becoming soft and squishy, becomes instantly liquid at right around 200 degrees. What it enables you to do, and when you look close up at something printed, you can actually see the individual lines or layers where that ABS

frosting was squeezed out and then melted down onto the next layer. Once printed, a lye bath is used to dissolve away any PLA support material. For example, when you have components that are fully meshed and to prevent those components from fusing together, you need to put a layer of something that is not ABS plastic in between them that you can then retrieve, which in this example is PLA. The lye bath will dissolve the PLA almost instantly. When you're actually preparing a model for printing, the model needs to be converted from AutoCAD or some other 3-D modeling format. The 3-D model is then converted into a series of 2-dimensional modes and rows because remember, you're squeezing out this frosting on a 2-dimsensal surface that's 10 thousandths of an inch thick. The chamber of a 3-D printer comes to a temperature of about 175 degrees Fahrenheit to anneal the layers that are deposited therein. I can speak with some authority to this because not only has UNR been working with 3-D printers for the better of 5 years, but the library that we are in was the first academic library to provide this as a service to not only students but members of the community at large to encourage the spirit of innovation.

I imagine the reason this technology is of interest to the board is the news a few months back about someone 3-D printing a gun and what are the consequences thereof. Can anyone in the garage begin mass producing weaponry? According to *Popular Mechanics*, the answer is not likely. *Forbes* also did a study asking how this is going to impact companies that actually manufacture weapons. How are these 3-D weapons going to affect the stock of gun manufacturers and the stock of producers of 3-D printers? The long and the short of it is the core problem is if your gun is printed out of plastic, the firing of the gun generates heat, and heat typically melts plastic. In fact, one of the first things I wanted to do was print a coffee cup in ABS plastic until it was pointed out to me that pouring a cup of 195 degree coffee would melt the cup. So, it probably would not be very practical to make a plastic gun. You're not going to have a plastic gun that is capable of firing off multiple rounds because you're going to generate too much heat. The liberator, which is the plastic gun that made the news, it does actually work. But, as a physicist and someone who has done more than his fair share of risky experimentation, there's no way I would test fire that plastic gun, even with a string and crouched behind a shield, because I'm pretty confident at some point that gun is going to come apart. The Darwin award is probably going to come into play. That said, it's entirely possible to generate one of these plastic guns in the near term. The future of manipulating 3-D printing lies not in the printer itself, but what is the printer printing with. In this scenario where the printing material is ABS plastic, it's problematic because you could get recycled plastic and turn it into 3-D printing material. So, you wouldn't be able to control the source material. You may be able to control it if you can control the manufacturers of 3-D printers in terms of overriding something in the software. For

example, when the printer is programmed to print something that resembles a barrel, the printer would stop printing. I don't think the technology is there yet, although it would certainly cost something to do it. The bottom line is that plastic guns, at this point, are really more of a proof of concept right now than something that's actually a risk at this time. That's not to suggest that there aren't things you could print that are dangerous. A problem I encounter regularly is that when you're printing at 10 thousandths of an inch thick, you can print a pretty sharp blade. So, we have really sharp edges and I sometimes clumsily cut myself. But, other than that, I wouldn't be alarmed about the ABS printing. I should also point out the costs associated with this. One of the advantages that I have at the university is I have kids working with me that are always several steps ahead when it comes to the next big thing. They were on top of this 3-D printing gun long before it made popular news. So, I asked them let's see how real this is, download the files and tell me how much it would cost a student or a community member to come in here and print the gun. We charge the cost of printing materials and it would have cost nearly $200 to print one of these plastic guns. You can find much cheaper firearms on Google than $200, so it's not very cost effective. Additionally, one might ask if a plastic gun would be useful if you wanted to slip past a metal detector, but this particular model of plastic gun has a metal firing mechanism, so it wouldn't get past a metal detector and it certainly wouldn't get past a full body scanner. But, it's something to have on your radar because it's just a little bit of metal, not a lot. So, it's worth paying attention to, but like I mentioned, it's not going to be cost effective in the near term as in 5 to 10 years.

A couple of things we are doing that may trigger some thoughts or questions: could 3-D printers be used to make custom drugs? Maybe at some point down the road that's a possibility. Not today. What we're dealing with today is a pretty caveman technology. You get ABS plastic hot enough until you can squish it out and control where it deposits and when it freezes, you've got something solid. You're not manufacturing the ABS that you're printing. An example that might help clarify this, you can Google "burrito bot" and there is a 3D printer that's capable of printing a burrito. It's not manufacturing the beans, meat, lettuce, etc. that goes into the burrito. Those are individual things that are extruded onto the burrito. So, when thinking it terms of molecules, you're not bonding a carbon molecule, to an oxygen molecule, to a sulfur molecule and coming up with something new. At some point down the road, that maybe possible, but for right now it's not even in the foreseeable technology. Rather, that's where the faculty members and grad students that I know that are trying to make their mark are desperately trying to figure out how we can develop this technology, but thus far are not having any success. In the meantime, you absolutely can print 3-D models out of ABS plastic of chemical molecules that you're trying to make sense of and trying to understand. One of the first

projects that came from us was a student in engineering who was able to realize his dream of this board game that involved particular pieces doing a particular thing and I heard he's actually in the process of negotiating the sell for the intellectual property of that game to be manufactured. We are also involved with STEM, science, technology, engineering and math outreach with the local high schools, so any of the local schools wanting to get involved with this, we have free access at UNR and the Dean of the college of Science is supporting a fair amount of that printing.

To be able to print something in 3-D, you have to start with a model that someone somewhere built that you are printing out. There are numerous 3rd party portals on the web where you can share these files. Of course this brings up copyright and patent issues, but so far what we're seeing are these open source communities on the web. So, thingyverse, for example, is a universe of things. It's a place where you can find literally hundreds of thousands of different models that people have created, uploaded and shared. So, you may download that file, since it's open source, modify it, print it, and then reload and share it. That's pretty much where we're seeing it now. A couple of other things that have been printed include, for example, mathematical art forms, some dangerous props for a particular game at Halloween, raspberry Pi cases, and sample holders such as flasks. A professor needed particular sample cases and asked that we fed ex them to him in Florida and we obliged.

One of the things that comes back to how we're operating in terms of printing, in the university system, we are always paying super close attention waiting for someone to snap or for something to go south and we need to immediately interject. And so, the 3-D printing is very much along those lines. The way we've been able to keep it as safe as possible is to keep it as open as possible. So, when you come in and want to print an object, your number one presenting that you have an intellectual property right to print that object. Then we're actually processing it on a computer screen right in front in the open in front of anyone that might be on the floor etc. of the library. Again, in every step throughout the process, the process is viewable to everyone around. The entire process is very public which is probably one of the most powerful tools in keeping something like 3D printing gun under control. I'll take any questions you may have at this time.

AG CORTEZ MASTO:
Dr. Colegrove, thank you very much. That is our future. That reminds me of the first time I saw the computer. Thank you. Very informative and very impressed with what you are doing. For my benefit, if I or any of the board members would like to see this in person, we can visit the UNR and see it, is that right?

DR. COLEGROVE:
Absolutely, we'd be profoundly honored.

Agenda Item 10 – Schedule Future Meetings and Agenda Items.

MS. SUWE:
Thank you Madam Chair. I'd like to set up a reoccurring date for meetings. Hence forth, all future meetings will be held on the first Thursday of each month divisible by 3. So, for example, our next meetings will be Thursday, September 5, 2013 and Thursday December 5, 2013.

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 3:35 PM.

Respectfully Submitted,

Belinda A. Suwe
Executive Director