MINUTES OF THE MEETING
OF THE
ASSEMBLY COMMITTEE ON JUDICIARY

Seventy-Sixth Session
April 29, 2011

The Committee on Judiciary was called to order by Chairman William C. Horne at 9:08 a.m. on Friday, April 29, 2011, in Room 3138 of the Legislative Building, 401 South Carson Street, Carson City, Nevada. The meeting was videoconferenced to Room 4401 of the Grant Sawyer State Office Building, 555 East Washington Avenue, Las Vegas, Nevada. Copies of the minutes, including the Agenda (Exhibit A), the Attendance Roster (Exhibit B), and other substantive exhibits, are available and on file in the Research Library of the Legislative Counsel Bureau and on the Nevada Legislature's website at www.leg.state.nv.us/76th2011/committees/. In addition, copies of the audio record may be purchased through the Legislative Counsel Bureau's Publications Office (email: publications@lcb.state.nv.us; telephone: 775-684-6835).

COMMITTEE MEMBERS PRESENT:

Assemblyman William C. Horne, Chairman
Assemblyman James Ohrenschall, Vice Chairman
Assemblyman Steven Brooks
Assemblyman Richard Carrillo
Assemblyman Richard (Skip) Daly
Assemblywoman Olivia Diaz
Assemblywoman Marilyn Dondero Loop
Assemblyman Jason Frierson
Assemblyman Scott Hammond
Assemblyman Ira Hansen
Assemblyman Kelly Kite
Assemblyman Richard McArthur
Assemblyman Tick Segerblom
Assemblyman Mark Sherwood

COMMITTEE MEMBERS ABSENT:

None

GUEST LEGISLATORS PRESENT:

Senator Barbara K. Cegavske, Clark County Senatorial District No. 8

STAFF MEMBERS PRESENT:

Dave Ziegler, Committee Policy Analyst
Nick Anthony, Committee Counsel
Jeffrey Eck, Committee Secretary
Michael Smith, Committee Assistant

OTHERS PRESENT:

Jeff Crampton, Private Citizen, Las Vegas, Nevada
Sam Bateman, Chief Deputy District Attorney, Office of the District Attorney, Clark County
Adam Stubbs, Government Liaison, Office of Intergovernmental Services, Las Vegas Metropolitan Police Department
Mark Lipparelli, Chairman, State Gaming Control Board
Warren B. Hardy, representing Switch Communications, Las Vegas, Nevada

Chairman Horne:
[Roll was called.] Good morning, ladies and gentlemen. We have two bills to hear today. We will take Senate Bill 376 (1st Reprint) first. Good morning, Senator.

Senate Bill 376 (1st Reprint): Increases the penalty for certain technological crimes. (BDR 15-1000)

Senator Barbara K. Cegavske, Clark County Senatorial District No. 8:
Good morning, Mr. Chairman and Committee members. Thank you for the opportunity to present S.B. 376 (R1) to you today.

As you know, Chapter 205 of *Nevada Revised Statutes* (NRS) contains our statutes for crimes against property, including unlawful acts regarding computers and information services.

[Senator Cegavske read from a prepared statement (Exhibit C).]

I have a witness in Las Vegas who would like to testify. His name is Jeff Crampton. He is here to testify about a serious crime that has happened to him. I would like to have this Committee hear about something that has not only happened over the last several years but is still happening today. Thank you.

Chairman Horne:
Thank you, Senator. We will go down south to Mr. Crampton.

Jeff Crampton, Private Citizen, Las Vegas, Nevada:
I have been a Las Vegas Valley resident since 1968. I am here today to share my firsthand experiences of having had my privacy violated, defamation of my name, been embarrassed, humiliated, intimidated, caused emotional distress, and terrorized by someone gaining unauthorized access to my email accounts and cellular phone.

[Mr. Crampton read from a prepared statement (Exhibit D).]

In the last six months, I have changed my phone number three times, and I change my email passwords weekly. Since the last time I testified for this, I met with somebody at the Federal Bureau of Investigation (FBI). I found out that changing your email passwords does not fix the problem. There is the capability for someone to go into your email account and select an option that will automatically forward any emails that you receive or send. So, even if somebody changes their password and there is no longer access to it, unless you realize this option is available, your emails are still being compromised.

[Mr. Crampton continued to read from a prepared statement (Exhibit D).]

Chairman Horne:
Thank you, Mr. Crampton, for your testimony. Are there any questions for Mr. Crampton? I see none. Mr. Bateman.

Sam Bateman, Chief Deputy District Attorney, Office of the District Attorney, Clark County:
I believe I first heard about what was going on with Mr. Crampton through Senator Cegavske when I was here during the 2009 Legislative Session. She was asking for a little help and advice. To some extent, I felt like I was ineffectual in helping Mr. Crampton because this has been going on for some period of time. For the current session, Senator Cegavske asked me what might be a reasonable response to some of the problems that Mr. Crampton was having. I located a particular statute, but let me back up.

I was attempting to figure out how to help local law enforcement in finding a serious enough crime that had been committed to justify their resources in investigating what is a very difficult crime to investigate. I think Mr. Callaway is there in Carson City. He can give you some sense of the resources it would take to investigate these types of crimes.

Initially, I had thought of a harassment statute. We make it a crime to harass someone. It is a misdemeanor until it becomes a threat of violence or a threat to one's life before it is a felony offense. So, I looked up NRS 205.477, which is a statute before you in S.B. 376 (R1). It provides, in section 1, that someone who causes denial of access to a computer system is guilty of a misdemeanor. Subsection 2 makes it a misdemeanor to gain access to someone's computer system without authorization. I thought that that was the most specific statute that I could find to address Mr. Crampton's ongoing problem at the time. I am not suggesting misdemeanors are trivial, but these types of crimes—identity theft and computer-related crimes—are so hard to investigate that local law enforcement has a hard time justifying putting forth the resources for, getting administrative subpoenas of Internet protocol (IP) addresses, and tracking these things down when the ultimate punishment is a misdemeanor.

I do not think that is the only reason that you ought to address this particular problem. I think that in this day and age, when we use our email and computer systems in the same way that we used the United States Postal Service in the past, this can be a very serious intrusion into someone's life. It is a very serious crime to interfere with the mail. I think we ought to consider whether we need to make it a more serious crime to intrude or to interfere with someone's email, which is essentially used now the same way we used to use the mail. So, I think this going to a category E felony in subsections 1 and 2, which is what this bill largely does, is an appropriate step to begin to address some of these problems. That is what I suggested to Senator Cegavske, and that is the bill you see before you.

Obviously, a category E felony means mandatory probation. It is likely that with the few cases where law enforcement is going to investigate these crimes and actually submit a case to the District Attorney's Office, as you know, we will be able to work with that E felony. Not everyone is going to be convicted of a felony necessarily, depending on their criminal history, but it at least gives us some leverage to address and stop the problem. If necessary, we will go forward and ask for that conviction.

This is not someone that Mr. Crampton just picked up off the street who has no criminal history and was just fooling around with his email. As it has turned out, over two years, we found out that this lady is quite a problem. She has another case in Las Vegas Justice Court where she was using the information of multiple victims to do things like gain electrical service at her apartment and pay for cable television, using their credit cards. She is also wanted in Arizona. We are not trying to target in any way someone who is sending out one lousy email. Because of the resource issues regarding these crimes, we investigate people who are really causing damage.

The only other change came on the Senate side. It was suggested by Chairman Wiener. In subsection 3(b), we added the "or attempted to cause" portion to what is currently a category C felony. That relates to when someone is hacking into your accounts or using your computer to do financial damage. This came up recently. This email harassment turned into the area of attempting to affect his financial situation. I think Senator Wiener asked if we want to wait until someone actually loses money before we get into the realm of a category C felony. She suggested, and I believe the Senate passed, the language you see in section 1, subsection 3(b). So, if someone breaks into your email to attempt to cause you monetary loss, it is a C felony.

That is the nature of the bill before you. I think it is a modest proposal to address this problem. I am happy to answer any questions.

Chairman Horne:
Thank you. We have a couple of questions. First is Mr. Carrillo, and then Mr. Frierson.

Assemblyman Carrillo:
How many people has this affected other than Mr. Crampton? Do you have records of how many people this has happened to? Is this just an isolated incident? I am sure it happens at different levels, but his case seems to be the most extreme. Do you have anything you can follow up with on that?

Sam Bateman:
That might be a good question to pose to local law enforcement. The way it works in my business is, local law enforcement investigates these crimes after they get a complaint. If they can put together a sufficient case, it would then be submitted to our office for screening, and we would decide whether to move forward. I do not see a lot of what I would call email hacking cases, but then again I do not see many identity theft cases, because they are so difficult. When we do approve them, they are very difficult to prosecute. I will defer that question to Mr. Callaway. I bet everyone in the room there has come home one day and opened up their email and found people responding to them, saying, "Hey, did you send me this spam?"

I think it is a very serious crime, even when it does not go to the extent to which it happened to Mr. Crampton. Hopefully, Mr. Callaway can answer your question.

Chairman Horne:
It is not Mr. Callaway; it is Mr. Stubbs.

Adam Stubbs, Government Liaison, Office of Intergovernmental Services, Las Vegas Metropolitan Police Department:
Assemblyman Carrillo, unfortunately, I do not have exact numbers for you related to the crimes about which you spoke. I can get those for you. I can tell you it is an emerging trend for our cybercrimes detail. We can only expect the number of cases coming to our department to rise over the next couple of years. I am sure it will go up substantially. With advances in technology, the advent of tablet readers, the iPhones, and the more access to emails and sources of technology that we have, I can only see the cases going up.

Assemblyman Carrillo:
Thank you.

Chairman Horne:
Mr. Stubbs, if you parse through much of Mr. Bateman's testimony, it seems to be that there is a lot of this crime going on, but at the currently misdemeanor level, it is not worth law enforcement's time to really pursue it. Do you find that to be the case?

Adam Stubbs:
That is correct. It is a very specialized area of investigation in our department. For that reason, it is a rather small detail. Within that detail, there is a lot of expertise and training. The cost and time associated with investigating these types of crimes are very substantial. We have administrative subpoenas, which are costly. We have the filing and submittal of search warrants for pieces of hardware that we need to access to obtain the IP addresses and other information that will assist our case. Currently, with the penalty set forth as a misdemeanor, we are unfortunately unable to give the resources and time that we would like to give the law merit. There are other federal crimes such as child pornography to which our detectives are able to give the time and resources to those cases because they are felonies. Because this law is currently a misdemeanor, it does not allow us to give the law the merit it really deserves.

Chairman Horne:
It sounds like you might need more resources as opposed to turning this from a misdemeanor to a felony. You are saying, "If it is a felony, we will enforce the law. If it is not a felony, we are not going to enforce the law."

Adam Stubbs:
Mr. Chairman, I do not think it is necessarily that we are turning a blind eye to the law. Would we love to have a larger cybercrime detail? Of course we

would. With the decreases to our budget, we are trying to tighten the belt all around our department. I do not think it is a matter of the detectives not having time to investigate this particular type of crime. I think that the entire investigation would be much better facilitated if we had a harsher penalty for these acts. As you heard from the witness, they can have long-lasting and devastating effects on the victims, and we would like to be able to send our submittals to the District Attorney and allow them the leeway and leniency to prosecute the crime they way they want to, as a felony, as opposed to just a misdemeanor. Most often, misdemeanors are not fully prosecuted to the fullest extent of what the harshest penalties of misdemeanor that are set forth in NRS allowed in court. By going with a class E felony, I believe it will allow us to charge the crime in the way that we think it should be charged. It is a very serious crime. We do not think a misdemeanor is the proper penalty for that.

Chairman Horne:
Mr. Frierson.

Assemblyman Frierson:
Thank you, Mr. Chairman. Mr. Bateman mentioned that harassment is currently a misdemeanor. I want to clarify. A second offense makes it a gross misdemeanor. I do not want to take this out of context, but it seems to me that this means that if somebody's ex-girlfriend has access and uses your computer twice, it is a gross misdemeanor, subjecting her to up to a year in jail. That is currently the law. We talked about misdemeanors, but no one talked about the gross misdemeanor. That is also an option, right?

Sam Bateman:
We would have to have that same investigation done for the harassment first offense, charge the defendant with first offense harassment, convict that defendant, than have it continue, and go through the same process for a second offense harassment that would upgrade it to a gross misdemeanor.

I have never seen one of these cases that has not resulted in the execution of some sort of search warrant. Very rarely, in my experience, have I seen misdemeanor offenses where the investigation involved either search warrants into people's homes or forensic analysis of their computers. If we could attack it that way, I absolutely would. That is the first thing I looked at when I was dealing with Mr. Crampton's situation. The harassment statute did not seem like the proper way to address that particular problem in this circumstance. I am not saying that it does not exist.

Chairman Horne:
Mr. Frierson has a follow-up.

Assemblyman Frierson:
We are talking about investigations and the resources necessary to thoroughly investigate them.

I have two points. Number one, its sounds like you are saying you do not believe that the resources you have are worth it if it is only a misdemeanor. Second, I realize that computer-related crimes are complicated, but I have seen numerous cases where it was fraud or child pornography, and they do not seem to have a problem tacking on multiple counts when they do one investigation, look at one computer, and see multiple uses of that one computer. So, if you can look at a computer and see that someone has accessed a site or an email address on multiple occasions, you have the option of charging as a gross misdemeanor and subjecting somebody to a year in jail and thousands of dollars in fines. Is that just something that you do not see as being worth the resources to do under the current statutory scheme?

Sam Bateman:
Let us say we were talking about harassment, which would be a misdemeanor for a first offense and a gross misdemeanor for a second offense. I do not think we can charge two harassments in one criminal complaint and call the first one a misdemeanor and the second one a gross misdemeanor. I think you would first have to be convicted of the first one and then resubmit a new case and charge it as a second.

That is my understanding of the law. I do not want to turn this solely into a resource issue. If this body does not think that people hacking into personal email accounts is . . . . If you are comfortable with that and what they might be able to do with that as being a misdemeanor, then that is certainly within the prerogative of the Legislature. I am suggesting that, as it stands right now, and based upon the nature of the crime and how much damage one can do by hacking into email accounts, then a misdemeanor is an insufficient penalty for that activity. If you think it is, then I certainly defer to you. We are bringing this to you. If you have other ideas that you think might be a better way to attack this type of problem, I am suggesting that, in this day and age, with what people can do, and how much activity people use their emails for, for someone to get in there and do the types of things that they can do, I think it is a more serious crime than a misdemeanor. By raising it to a felony, you get the benefit of a higher priority on the list of crimes that local law enforcement has to address on a daily basis. I do not want to suggest that that is the only reason. We are here because what this lady is doing to Mr. Crampton, and what others can do, is very serious to what people are now using more and more for all portions of their daily lives to include personal communication to

business activity. That is why I think it is an appropriate increase to a category E felony.

Chairman Horne:
Thank you. Ms. Diaz.

Assemblywoman Diaz:
Mr. Crampton, at what point in time did the FBI start taking a role in investigating the lady who hacked into your computer and email?

Jeff Crampton:
Thank you for asking that. First of all, there was a question raised about how often this happens. The FBI special agent that I spoke with let me know that this happens so often—thousands of times a day. They have a website—Internet Crime Complaint Center (IC-3)—specifically to make complaints regarding people hacking into your email and gaining unauthorized access.

As far as my contacting the FBI to get them to pay attention or to find out if there was any remedy through them, because there did not seem to be one for me on a state or local level, I was told pretty much the same thing: They are looking for child pornographers. They gave me some good information regarding what I could do. They let me know that this woman was under investigation for other Internet crimes. She has presented herself as a music promoter and run a scam through a website for musicians across the country, telling them that she was going to get them booked at a venue and recorded to a compilation disc, and they just needed to send her $300 to $500. They would do that, and of course, nothing would happen.

She has been doing this for years. If I were to share her name with you and suggest that you might Google her, you would find pages and pages of these complaints. This is the reason that the FBI is currently investigating her for other Internet crimes, but not specifically for my complaint.

Assemblywoman Diaz:
Thank you.

Chairman Horne:
Mr. Sherwood.

Assemblyman Sherwood:
Thank you, Mr. Chairman; and thank you, Mr. Crampton, for coming forward. I know it is kind of a bad prank gone badly, and I certainly can empathize with you on that.

As a preface to this, there are two issues. I think we are talking about bringing the penalty on par with the real world. The virtual world and the real world are now the same, right? So, to be on par, if you were to break into a mailbox or if you were to break into a house and go through the filing cabinet of a personal business, this is what we are talking about.

The other thing would be with the penalties now in other states, it seems to me that Nevada is a little slow on the curve as far as collective cyber use. So, our Internet penetration is lower than that of California and Washington. Craigslist was late getting here. I am not trying to explain away our statutes, but I think it is natural that we are behind the other states because our Internet penetration lagged. We are catching up, so please do not disparage us for being behind.

To law enforcement, the reason we have different penalties is for a deterrent, right? Did we miss that in this whole debate? Some of these should be category B felonies, based on other similar crimes, but is that for deterrence? I heard that in Mr. Crampton's testimony, that she kind of stuck out her tongue and said, "You cannot touch me," right?

Adam Stubbs:
Although that is not our number one priority for wanting to make a harsher penalty, of course trying to make a crime less attractive to a criminal based upon a harsher penalty is always a benefit for law enforcement. I do not think that there is any denying that having a harsher penalty for these types of crimes would dissuade some of these people from taking part in these kinds of acts in the future.

Assemblyman Sherwood:
It is almost a self-evident point, but it seems we have lost it in this debate.

Chairman Horne:
Do you have a question, Mr. Brooks?

Assemblyman Brooks:
Yes. Thank you, Mr. Chairman. Mr. Bateman, you stated that you did not know if this body was comfortable with people hacking into email accounts. I do not know if I am comfortable with that. I think I am more uncomfortable with the fact that you are not currently using the tools that you have to

apprehend individuals that are harassing people like Mr. Crampton. Is it really the case that you are not apprehending individuals because it is only a misdemeanor? And if so, how is making it a felony going to give you any more resources to do what you need to do? That is question number one.

The second question is, would this also apply now to major companies, nonprofits, and whatnots that have their systems hacked? Based on the bill, it seems to include that as well. I think I am more interested in that type of behavior, because that is on a different level for me and a little more serious. Thank you.

Sam Bateman:
As far as how law enforcement chooses to divvy up their resources, I cannot speak to that. I get it on the back end once they have investigated it. I very rarely see the type of investigation that would be required for this type of crime to go into something that is a misdemeanor. It is very significant.

Some of these types of crimes we have currently are up to category B felonies, and carry up to 20 years in prison for obtaining and using personal identifying information for one means or another. The Legislature decides what the appropriate penalty is. If you have 100 crimes and you have x number of dollars, any local law enforcement has to decide how they utilize those resources. That is one component of it.

I think the first component of it is what I was referring to as your prerogative to decide whether this type of crime is serious enough to warrant felony treatment. I think Mr. Sherwood made a good point that any other crimes in this arena are already felonies.

As to your second question, Mr. Brooks, I think that with the way the statute is currently written, it probably would have something to do with commercial entities and accessing their particular information. I think that exists in law. I have never seen too many cases like that, where we have had commercial entities that have been hacked into. My guess is that if someone was trying to hack into a commercial entity, it would probably be more for the purpose of financial gain. I am speculating on that. That already exists in statute, absolutely. I would think that that would probably come under subsection 3, which also includes interrupting or unlawfully accessing public service, such as your power company or your gas company.

At some point in this very statute, we recognized the seriousness of these types of acts when we make it a category C felony. We just made that specific to public utility entities, or to do damage to one's finances.

Assemblyman Brooks:
Actually, I want to know, based off this bill, if someone were to deliberately plant a "bug" in a system to keep it from working, would that also be considered part of this bill, or is it just the theft of identity and using the personal information?

Sam Bateman:
Section 1, subsection 2, which is already in existence, states that if you willfully and without authorization did what you just said, I think that that would be a category E felony. Currently, it is a misdemeanor; however, under subsection 3(c), if it was designed to cause an interruption or an impairment of a public service, then it is already a category C felony. We would not be affecting the statute.

Assemblyman Brooks:
Thank you.

Chairman Horne:
Mr. Frierson.

Assemblyman Frierson:
My discomfort with what we are discussing right now is the opportunity for it to be applied in an extremely broad manner. For example, say someone uses my computer to check their web-based email account, and they do not log out. The next day I open it up to check my email, and it comes up with their email address, and it happens to be my ex-wife. Now I am potentially subject under this. I am not concerned about it being used to protect people like Mr. Crampton, who have clearly gone through some extreme harassment that has impacted his life, but I am concerned about all the other people who could be subject to this in the midst of what are often ugly breakups.

Mr. Bateman, I think you mentioned obtaining personal identifying information of another. *Nevada Revised Statutes* (NRS) 205.463 provides that any person who knowingly obtains personal identifying information of another person and uses that information "1(b) (1) To harm that other person; (2) To represent or impersonate that other person to obtain access to any personal identifying information of that other person without the prior express consent of that other person; (3) To obtain access to any nonpublic record of the actions taken, communications made or received by, or other activities or transactions of that other person" is already a category B felony. I do not see why we cannot use existing statutes to protect somebody like Mr. Crampton. From what he has described, that fits exactly within that statute and is already a category B felony. So, we could use that statute to protect people like Mr. Crampton who

have legitimate grievances and need to be protected without Jack and Jill's argument becoming a felony because somebody checked the other's email after they broke up. That is my concern, and I am not entirely sure why this statute would not apply.

Sam Bateman:
I believe that statute applies specifically to personal identifying information of another person, and I think there is a definition of that. I do not know if you have it handy there. I do not have it in front of me.

With Mr. Crampton's situation, it may very well at some point have worked its way into that particular statute. I think it probably would not have applied early on. I remember looking at that statute. I think that was more specific to the personal identifying information of another, which is probably included with a definition in either NRS 205.463 or 205.461, which is a category D or C felony. Sometimes those two statutes are a little confusing.

As to your first point, I do not disagree that we can encompass many of these statutes. If applied literally, and with all the resources in the world, we could encompass the wrong type of people or the people we were not looking for. We are talking about the difficulty in investigating these crimes. I wish we could legislate out all the unintended consequences of every crime we have in our penal statute. I do not know what to tell you or what the solution to that would be, other than what currently exists as law enforcement and prosecutorial discretion. Under the circumstances that you were suggesting, you would have to be mad at your ex-girlfriend, go down to the police station, file a report that says she checked her email on your computer and that she did not have authorization, and the police would have to investigate that situation. If they decided that a crime had in fact occurred based on your complaint, they would have to then submit it to our office. We would then have to decide whether we would prosecute that case or not. That exists on most crimes, but I do not know the best way around that.

Assemblyman Frierson:
If I could clarify, NRS 205.4617 defines "personal identifying information," and a password is one of the definitions.

Chairman Horne:
Thank you. Mr. Brooks.

Assemblyman Brooks:
Thank you, Mr. Chairman. My colleague has expressed concern with statutes that already exist. I am reiterating this. That is my concern, that laws already

exist that should protect someone like Mr. Crampton. I am more concerned why something was not done earlier in his case and why it got to the point where we would have to create law for such a situation. Are we just putting something else on the books that will not be enforced? I think it is important that we protect people with email, but I wonder, if you are not doing it effectively now, what is going to change?

Chairman Horne:
I will take that as a statement and a rhetorical question. Mrs. Diaz.

Assemblywoman Diaz:
Thank you, Mr. Chairman. Mr. Stubbs, at what point in time do the law enforcement agencies take an active role in these cases where, using computers, a person is wreaking havoc in someone's life such as in the case of Mr. Crampton?

Adam Stubbs:
Most often, we have a victim who comes into one of our stations and files a report. The report is taken under whatever NRS that either a civilian or an officer can determine was violated. That report is then sent out to the specific detail under which the crime falls. In this case, it may be sent to our General Investigations Unit or sometimes maybe our Fraud Unit. Once those detectives can determine that there is a specific technology-related element within the crime that was committed and that might require the assistance of forensic analysis or the special skills of our Cyber Crimes Unit, it could pass hands within the department, and it will ultimately end up in the proper detail that investigates these types of crimes. It is then up to the detectives in that detail to determine, using their best discretion, whether the crime that was allegedly committed falls under the specific NRS that the report is taken under. Sometimes we will find an alternative NRS that the crime would fit better under. As far as changing the law, this law is already here. It is in NRS. It is a specific NRS that responds to technology-based crime. We would most likely use the NRS that best applies to the crime committed.

In response to your original question, it would go through the normal chain of reporting. It would end up in the proper detail, usually within two to three business days. At that time, they would start their investigation, contact the victim for further information, and start the subpoena process for records, or search. They have to establish a suspect before they can start subpoenaing records and submitting search warrants for hardware. There is a lot of red tape that we may have to navigate through with these types of investigations. It can take a while.

Assemblywoman Diaz:
Did Mr. Crampton come to law enforcement and try to file to get an investigation underway? I am curious because it seems like nothing was done on the law enforcement end, and so now he is seeking a way that other people can be further protected. I did not hear in your testimony that you consider the level or the degree of the penalty when you are going to undertake an investigation. I know you check with statute, but to what point does his situation have to escalate for the law enforcement agency to take part?

Adam Stubbs:
I do not know Mr. Crampton's personal case. I would be happy to get with him and follow up with the detectives he has worked with. I am not trying to make it sound like it is a resource issue. We feel as a department that this type of crime is very serious, and we think that the change in penalty of this law will give the law the merit it deserves, not so much that it allows us the additional time and resources to work it. We feel that the misdemeanor is not only failing to keep criminals from doing this in the future, but also the increase in penalty will assist with the penalty being harsher and allowing him to have the justice he deserves in court. Unfortunately I cannot speak on his specific instance. I wish I could, and I would be happy to work with him to see if we can maybe follow up and get his case back on track.

Assemblywoman Diaz:
I appreciate it. Thank you.

Chairman Horne:
Is there anyone else here in Carson City wishing to testify in favor of S.B. 376 (R1)? Is there anyone in Las Vegas?

We will move to the opposition. Is there anyone here opposed to S.B. 376 (R1)? Is there anyone in Las Vegas?

Is there anyone here or in Las Vegas wishing to testify in the neutral? I see none. Before I close, I will allow a final comment from Senator Cegavske.

Senator Cegavske:
I want to thank this Committee for the thoughtful conversation and comments about this piece of legislation, and I would appreciate your favorable consideration. Thank you.

Chairman Horne:
Thank you. I am going to close the hearing on S.B. 376 (R1), bring it back to Committee, and open the hearing on Senate Bill 218 (1st Reprint).

Senate Bill 218 (1st Reprint): Revises provisions governing the regulation of gaming. (BDR 41-991)

Good morning, Chairman Lipparelli.

Mark Lipparelli, Chairman, State Gaming Control Board:
Good morning, Chairman Horne and members of the Committee. Senate Bill 218 (R1) is in its first reprint dated March 3. There are several sections that I can cover in summary for you. We will then come back to any questions you might have.

The series of changes that we are recommending address a number of potential opportunities and issues that we at the State Gaming Control Board come in contact with on a fairly regular basis. The first one relates to the definition that I will cover later in an area called "service provider."

Section 2 of the bill relates to the addition of language in law that would allow for the definition of a location called a "hosting center." With the advances in technology and casinos, many operations and technology providers are seeing the benefits of colocation facilities. Much of what is required in law today would mandate that a casino operator house their technology equipment on the premises. The hosting center concept would allow for those locations to either, through a third party or they themselves, locate their technology equipment somewhere other than the premises of a nonrestricted location.

Coming back to the original definition, section 3 adds another definition to our law in an area called "service provider." This is what I have been describing as an "in-between" level of licensing and review. Today, on the technology side, there is a fairly expensive and lengthy process to become a manufacturer of gaming equipment. As the industry changes and evolves, there are several potential new entrants to the business that might have modules or provide a different level of service far short of a gaming device or a ticketing system, or something for which we require full-blown licensing. In many cases where it touches things like a cashless system or the random number generator of a slot machine, we are puzzled and do not really have an opportunity to provide flexibility to somebody like that. So, we are creating a classification called a service provider that would allow the Board the flexibility to deem someone a service provider and potentially require full-blown licensing where necessary, or in other cases, potentially just registration as opposed to the cost and energy associated with a full-blown licensing.

Sections 4 and 5 of the bill are what I would call ministerial, for the most part. Section 4 would not require the Gaming Commission to approve the

day-to-day operational activities and functions of the Board, such as our personnel manual. They have no day-to-day interest in that. Historically, that personnel manual sat unrevised for a period of 10 or 12 years, just because of the difficulty of composing changes and getting in front of the Commission. I spoke to the Chairman of the Commission, and he expressed his desire that that be done at the Board level.

Section 5 of the bill relates to the publication of various things that we put out to the public. We can do that through our website very effectively and meet the requirements of posting for the public.

Section 6 of the bill relates to another housekeeping matter—the number of times we have to come back and get approval for something that is basically already approved by the Legislature in our revolving account.

Section 7 is an important change with the bankruptcies and some of the reorganizations that have occurred. One thing that has really tested the Board's staff is the requirement that they come back before the Board for an audit when potentially that location might have been audited three, five, or eight months previously. This would allow the flexibility of the Board and Commission to deem a location to be a continuing operation and not require an iterative audit process, so that if a location was changing either its corporate structure and it is substantially similar to what it looked like before, we could deem that location a continuing application and pick them up on our normal audit schedule and not interrupt our audit process. This was brought to light in the last two years with the number of bankruptcies. We would have to reallocate all of our audit resources to potentially picking up what we called a "closing audit for a change of control" when the entity looks substantially similar after their reorganization to when they went in.

Sections 8 and 9 are similar. This makes Nevada more like the rest of the world with respect to private companies and the requirement for licensing. This would allow for those parties under a 5 percent threshold to not be required to file. Today, there is a 0 percent threshold. We are fairly unique in that 5 percent has become a pretty common standard that trips the trigger for someone to have to file, so this has potential benefits in many different areas for companies that want to raise capital. Today, those limited liability companies (LLCs) and limited liability partnerships (LLPs) do not have the flexibility of raising private capital compared to their peers, who are public entities and who would not require licensing of any individual under 5 percent. In these trying times, from a financial perspective, that investment by someone who has no desire to control the operation just for investment purposes would subject them, at a 0 percent threshold, to licensing of even one share of a location.

Section 10 is another efficiency gain that we have been working on through regulation that would require this change in statute. All filings to the Securities and Exchange Commission (SEC) must be in Electronic Data Gathering Analysis and Retrieval (EDGAR) format. Those "EDGARized" forms are available 24 hours a day, 7 days a week on the SEC website. This is somewhat of a victim of time. Years ago there was a requirement that those companies file those hard copy documents with us. That has long since passed its usefulness. Our staff can access those files anytime they wish online. This bill would actually remove that requirement, and we would cover that through a change in our regulation if it were to pass. Section 11 deals with the same change.

Section 11.5 relates to the service provider licensing structure that I talked about earlier.

Section 12 of the bill provides some clarification with respect to what is prohibited under the law today, relating to equipment that might be used to project the outcome of a game or something used principally by our law enforcement group to make arrests of people trying to cheat slot machines. There are, and have been, several requests by the industry to create game programs that could be approved by the Board and Commission that potentially would be violative of those kinds of activities, but it is essentially part of the game. We are suggesting that, when approved by the Commission, those kinds of devices may be used when they are part of the game as approved by the Commission and to clarify that when those devices are approved, it is not a violation of criminal statute.

The last relevant section is section 14, which relates to the Regulation 6A cash transaction and recordkeeping that has essentially trapped a small portion of our budget. Regulation 6A is no longer a requirement by the state. It is handled by the federal government, so we no longer have a need for this funding. This would allow us to remit those funds back to the state.

Those are the summaries of the items contained in the bill.

Chairman Horne:
Thank you, Chairman. I do not see any questions, but I have some. In section 2, subsection 2, where there is the new language ". . . the Commission may, with the advice and assistance of the Board, provide regulation . . . ," I do not understand why we would not say "shall . . . provide regulation."

Mark Lipparelli:
Mr. Chairman, I have no objection. That language could be "shall." I would certainly stipulate to that change. We think this is a positive change for industry, so we fully intend to proceed with regulation development.

Chairman Horne:
I would ask that also in section 3, subsection 2. That first "may" could be changed to "shall." Also, in section 4, you strike "with the approval of the Commission." Historically, the Board has gone through the Commission for, you said, solely administrative purposes. Is that correct?

Mark Lipparelli:
That is right.

Chairman Horne:
Section 5, subsection 1(a) changes the notice requirement. You have it now where it is at least 30 days before meeting, but you have deleted "20 days before any subsequent meeting." I am envisioning a scenario where you give notice that you are going to speak on a particular issue, but that issue may not get resolved, and you will have a subsequent meeting, but then no one is put on notice that you will continue to address that issue.

Mark Lipparelli:
The practice of the Board is that we always public notice all of our workshops related to the adoptions of regulations. We are subject to the Open Meeting Law. I think the answer to your question would be that any subsequent meeting relating to the discussion of the adoption of a regulation is part of our posting process. Unless I misunderstood your question, I do not think there would be a case where an individual would not have public notice of the consideration of any regulation change.

Chairman Horne:
What was the purpose of striking "20 days before any subsequent meeting?"

Mark Lipparelli:
I do not know the answer to that, Mr. Chairman. It has been my experience for as long as I have been affiliated with the Board and sitting on the Board that we have always had the public notice requirement. This may have been a legacy of the past where there might have been follow-ons. We had this come up in a meeting last week where if the meeting was continued more than three days, then it required a reposting under the open meeting law. I guess my confidence level was fairly high that there is not a case where we run into the issue of not having a public posting.

Chairman Horne:
In section 6, subsection 4, you strike out the requirement of presenting a claim to the State Board of Examiners after an expenditure of money from a revolving account. What is the purpose of that?

Mark Lipparelli:
It has been explained to me that what has essentially happened is that this has never been an issue for the Board. I believe the practice of the Board has been that it has never come up as an issue, so they were recommending that once the funds were allowed, the Board has always returned the money to the state. It has never been required.

Chairman Horne:
If we could move to section 7 where it removes the requirements that certain business entities must incur before licensing, and "may be deemed transferred." Could you again give us instances on how that happens and why we are deleting that?

Mark Lipparelli:
Certainly. Our licenses may be reissued. They are not generally transferrable. You cannot give your license to another party in a transaction without the approval of the Board. Oftentimes, in the case of reorganization or a bankruptcy, which has been fairly prevalent in the last couple of years, the nature of the business is essentially the same. The same group of owners are going through a reorganization, although that will generally result in a new license being issued, so you might have a location that, for all other intents and purposes, looks and feels exactly the same in its different form. The issuance of a new license triggers and mandates that our audit division conduct a closing audit of that first location before it can become the second location. Oftentimes those are unplanned, and they consume a great deal of time. The worst case scenario would be if we just concluded an audit of a location in our regular scheduled cycle, that period of time may only be six months. From our perspective as an agency, without the ability to deem something a continuing operation through good reasoning, because it is in the law that we must count it as not a continuing operation, it is fairly inflexible. We would have to scramble our audit resources to conduct a short tem audit when we might have just concluded one six months earlier. The view is that in large measure, it serves very little purpose, and we would rather have the flexibility to deem something a continuing operation and provide that flexibility which section 7 provides.

Chairman Horne:
Further in section 7, subsection 2, there is new language that reads "The Chair of the Board may refer a request for administrative determination pursuant to

this section to the Board and the Commission for consideration, or may deny the request for any reasonable cause. A denial may be submitted for review by the Board and the Commission in the manner set forth by the regulations . . . which pertain to the review of administrative approval decisions." It seems that gives a tremendous amount of power to the Chairman to unilaterally deny requests. Why are we making that change?

Mark Lipparelli:
The exchange here is, that for those entities that would formally have to have met the prescriptions included in the law, we also want the protection against those similar entities coming to the Board and essentially forcing the hand of the Board to say, "We are deeming this in our own minds a continuing operation, and you must deem it such." We would want to have flexibility for the Board to say, "You are pushing the envelope of what is a continuing operation." We have this in other areas where, when the Board or the Board Chairman believes that something deserves the policy-shaping discussion at the Commission level, the Board Chairman has the ability to say, "We disagree. We think you are not a continuing operation. The changes are so significant, and if you do not like the answer, we can provide that opportunity to you in forum at the Commission level, and you can make your argument." It is a two-tiered approach in that if the Board does not agree, they can make their argument before the Commission.

Chairman Horne:
In sections 8 and 9, where we are talking about the LLPs and the percentage, in your statement you were saying how there was not much concern if somebody has a minimal amount of percentage into a property, they have to go through the full licensure procedure. But, what if you have a family? Let us say the front row of Committee members are a family. Each of them has 3 percent of their own. Does the Board or Commission investigate that?

Mark Lipparelli:
Central to the argument is, this is for the purposes of someone who wants to be passive to the extent that it is the interpretation of the Board that someone is trying to aggregate—in a sense, gain control. The central theme of all of our statutes and regulations relate to control, so this would not avail them the flexibility they would be requested to file. This basically addresses the similar opportunity the public company investors have in our state today, where you could acquire beyond 5 percent without being licensed. The same thought process is engaged here. If you had a passive investor who had no interest in exercising control, the 0 percent threshold would be pushed up to 5 percent. But, if you were doing it for the purposes of acquiring control, or if it was for

any other reason deemed to require licensing, the Board retains that power. It just pushes the threshold from 0 to 5 percent.

Chairman Horne:
So, if Mrs. Diaz were the matriarch of this family here, you would see on these various applications of all these different family members who has passive levels of control. Would you investigate that and the control that Mrs. Diaz has over the rest of her family members who have small percentages?

Mark Lipparelli:
Certainly, Mr. Chairman. The burden is on the applicants to demonstrate their cause. This is not a given. They have to demonstrate that they are independent and passive. That is a test that we evaluate, and not the other way around.

Chairman Horne:
Mr. Brooks.

Assemblyman Brooks:
Thank you, Mr. Chairman. Mr. Lipparelli, can you give me an example of when you would need to use a device to predict the outcome of a game?

Mark Lipparelli:
I actually have one that became the genesis of this request. One of the creative game makers wanted to include in their idea a bluff feature in a table game. A lot of debate went back and forth about whether a bluff feature and how it was composed would, in the historical terms of this, project the outcome of a game or keep track of cards. We went back and forth about whether that was violating the statute. There are a lot of creative ideas in game play, where a set of odds might be created by having knowledge of what has been played or having a knowledge of what might be the outcome of a game to change and make a bet offering, as long as that is not providing a disadvantage to the house or the player. It may be that a certain number of cards have been played out of a deck, which changes the composition of the future odds outcome of a game, and which may give the creative entrepreneur the ability to create another set of betting opportunities, given what is left in a deck of cards. In doing so, that is allowing for good. It is being used for good, as opposed to being used for bad. This statute is designed to catch people cheating the house, or the other way around—catch the house cheating the player. The context changes when using an approved device by the Commission. That is not a problem. That is why we are trying to clarify it.

Assemblyman Brooks:
So then, you would use these types of devices all the time, because to determine the odds you would have to use some type of device to determine those odds.

Mark Lipparelli:
Yes, and that is why we included the part ". . . may be made available of an approved game . . . ." The burden is on the applicant to demonstrate the quality of the product and how it is being used but maintain the integrity of what is being prevented, which is people taking advantage of the house or vice versa.

Assemblyman Brooks:
Thank you.

Chairman Horne:
Are there any other questions for the Chairman? I see none. I will open it up to anyone else who is here to testify in favor of S.B. 218 (R1). Is there anyone in Las Vegas? Mr. Hardy.

Warren B. Hardy, representing Switch Communications, Las Vegas, Nevada:
I have with me Mr. Sam Cantor, who is the Associate General Counsel for Switch Communications, and Mr. Darren Adair, who is the Chief Financial Officer. Many of you are familiar with Switch Communications, which is one of Nevada's star technological groups. We are certainly pleased to have them here.

We are here today in full support of S.B. 218 (R1). There is one section in the bill that gave us pause. We have had conversations with Chairman Lipparelli, and we very much appreciate his willingness to clarify for the record what the intent of the Control Board and the Commission is on this. Specifically, I am addressing section 2, subsection 4(b) of the bill. That starts on line 17 of page 4 of the bill. This is in the section that indicates that the Commission will adopt regulation and that, pursuant to this section, they must first define a hosting center, and then—and this is where we are seeking some clarification for the record—"(b) Provide that the premises on which the hosting center is located is subject to the power and authority of the Board and Commission pursuant to NRS 463.140, as though the premises is where gaming is conducted and the hosting center is a gaming licensee." Based on our conversations with Chairman Lipparelli, we clearly understand that the intent is that there would be unfettered access for the GCB to these facilities. We were a little concerned that this might be interpreted at some point to mean that it is the intent of the Legislature that the regulations require that hosting centers be licensed as

gaming licensees. We would very much appreciate the opportunity to have Chairman Lipparelli speak to this and perhaps clarify the intent before your legislative record.

Chairman Horne:
Thank you, Mr. Hardy. Chairman Lipparelli, is that section supposed to be "as if," basically?

Mark Lipparelli:
Mr. Hardy is correct. The intention of the Board is to certainly bring life to the notion of having information technology (IT) centers and IT architecture exist somewhere other than the premises of a casino, and that may be through third parties or licensees who actually conduct those kinds of activities on their own off-site premises. It is not intended to mean that just because someone is engaged as a third party to conduct these operations that that would subject that party on its face to licensing. This does provide for that eventuality if it is deemed by the Board that these people are serving in some significant capacity where we might want to call them forward for suitability, but it is not the intention. The intention is that these third party facilities could exist. They would go through a registration process, but it would not require them to be licensed. That was clearly our intention. At least with the way it is written, I believe that it says that, but if we want to work together to make a change to make it more clear, then I am happy to do so, but I think our intention is clear enough.

Chairman Horne:
Thank you. Mr. Hardy.

Warren Hardy:
Chairman Horne, we certainly are not requesting an amendment, unless you think it is necessary. We are very pleased with that explanation for the record. Thank you very much.

Chairman Horne:
Thank you, Mr. Hardy. Are there any questions for Mr. Hardy? I see none. Is anyone else in Las Vegas wishing to get on the record in favor of S.B. 218 (R1)?

We will move to the opposition. Is there anyone opposed to S.B. 218 (R1) either here or in Las Vegas? Is there anyone in the neutral position? I see none. Chairman Lipparelli, do you have final comments you want to place into the record?

Mark Lipparelli:
I have none, Mr. Chairman.

Chairman Horne:
I will close the hearing on S.B. 218 (R1) and bring it back to Committee.

That concludes our business for today, unless there is any other business to come before the Committee. Seeing none, we are adjourned [at 10:33 a.m.].

RESPECTFULLY SUBMITTED:

_____
Jeffrey Eck
Committee Secretary

APPROVED BY:

_____
Assemblyman William C. Horne, Chairman

DATE: _____

EXHIBITS

Committee Name: Committee on Judiciary

Date: April 29, 2011 **Time of Meeting: 9:08 a.m.**

Bill	Exhibit	Witness / Agency	Description
	A		Agenda
	B		Attendance Roster
	C	Senator Barbara K. Cegavske	Prepared Statement
	D	Jeff Crampton	Prepared Statement