TECHNOLOGICAL CRIME ADVISORY BOARD
Technical Privacy Subcommittee

MINUTES OF THE MEETING

August 29, 2014 at 1:30 PM

VIA VIDEO-CONFERENCE
Office of the Attorney General
100 N. Carson Street, Carson City, Nevada 89701
And
Office of the Attorney General
Grant Sawyer Building
555 E. Washington Street, Suite 3315, Las Vegas, Nevada 89101

1. Call to Order and Roll Call.

Hal Berghel, Chair; James Elste; Ira Victor; Stephen Bates Dennis Cobb.
Not Present: James Earl; Allen Lichtenstein. A quorum was established.

2. Public Comment. (Discussion Only) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

There was no public comment.

3. Chair's Welcome. (Chair)

Mr. Berghel welcomed the members to the fifth meeting of the Subcommittee.

4. Report on Technological Crime Advisory Board meeting of June 5, 2014, and status of approved resolutions for Technical Privacy Subcommittee.

Mr. Berghel stated that the Subcommittee's resolutions were discussed at the Board meeting. There was some opposition to the proposals from the representative for the Clark County Sheriff and from Senator Ford. The Sheriff's representative was uneasy with any proposal increasing the protection of privacy without studying the full ramifications in regards to police investigations. Mr. Berghel asked for Mr. Kandt's assessment.

Mr. Kandt reviewed the four proposals made by the Committee:

1) To amend the news shield law.
2) To add the word "privacy" to the Nevada Constitution.
3) To seek a joint resolution from the Nevada Legislature to call upon the federal congressional delegation to look at expanding privacy protections at the Federal level.

4) The proposal to amend NRS 179.045 to permit the application for and issuance of search warrants by electronic transmission.

He reported that the Board did not endorse the first three proposals. With regards to the news shield privilege, the representative from the Nevada Press Association was there and indicated that 90% of his people are already covered and he was reticent to opening up the statute to try to cover the other 10%.

With regard to all three of the proposals not endorsed by the Board, the biggest concern was whether these proposals were outside the Board's statutory scope. The fourth item, they believed, did fall within their scope and they did endorse it. They will support amending the search warrant statute provided there are appropriate protections and precautions. The proposal has been included in a bill draft request in the Attorney General's legislative package that was submitted to the legislature.

Given the concerns that the other proposals were outside the statutory authority of the Board, Mr. Kandt suggested that, because the work of this Subcommittee is so important, perhaps it should be created as a stand-alone advisory board to look at all issues regarding digital and technological privacy. Mr. Kandt stated he had spoken to Assemblyman David Bobzien, and they had discussed the idea of having the legislature create a separate advisory board to look at technological and digital privacy. Assemblyman Bobzien was very receptive to the idea and said he would be willing to put in a bill draft request to create an advisory board. Mr. Kandt stated that digital privacy is the major civil rights issue moving forward and it would be appropriate to have an advisory commission to study issues and make recommendations to the legislature.

Mr. Berghel stated that the original proposal he had made to the Attorney General two years ago was for a board to make recommendations to the Attorney General and somehow it got changed so that the Subcommittee reported to the Board.

In regards to the first three proposals, Mr. Berghel stated that the Board never took action on them; rather\\, the Attorney General as chair tabled them. He clarified that it was Senator Ford—not the entire Board—who stated his concern that the privacy resolutions fell outside the Board's statutory authority. Otherwise he agreed with Mr. Kandt's assessment.

Mr. Elste thought the results of the Board meeting were disappointing. He was concerned that the Subcommittee has spent the better part of a year on the proposals and had pulled together a group with expertise in the field who are able to give good counsel. With three of the proposals tabled, it concerns him that the group may feel that their efforts are not appreciated and that their time is better spent elsewhere. It is important for Nevada to have a body whose responsibility is to look at privacy issues. He agrees that this is the civil rights issue of our age. The issues are complicated and it takes people who are focused on privacy issues in the digital age to unravel them. He stated that perhaps the question is about the future of the group and expressed hope that it can find a better structure or attachment point so it can advance its agenda and continue with its mandate to examine privacy issues.

Mr. Victor agreed that this Board needs to exist separately, and that the issue is an important. Nevada needs to be on the cutting edge for the sake of the public, businesses and technology in Nevada.

Mr. Kandt added that Mr. Berghel is correct in his clarification of Mr. Kandt's summary of the meeting. It's not that the entire Board was reticent to take action, but Senator Ford expressed the greatest concern about the Board acting outside its statutory authority. The Board was created in 1999 and the current implications of digital privacy and developments in technology were not yet envisioned.

Mr. Elste observed that under NRS Chapter 205A setting forth the Board's duties, duty #5 is to "Evaluate and recommend changes to existing civil and criminal laws relating to technological crimes in response to current and projected changes in technology and law enforcement techniques." He argued that under that part of the statute, the Board is not acting outside of the bounds of its statutory authority.

Mr. Kandt stated that as the Board's Executive Director/General Counsel and by extension, the Subcommittee's General Counsel, he had never voiced any concern regarding the topics the Subcommittee considered and the recommendations they made because he also interpreted the statutory scope in the broadest way possible. But there were Board members with that concern and that is why he wanted to look at creating a separate advisory board dedicated just to the issue of technological and digital privacy. He suspected that there will be many legislators in addition to Assemblyman Bobzien who will be interested in it.

Mr. Victor added that in the last few months the Nevada Supreme Court has adopted new rules of civil procedure related to electronic information. They are using standards from the Sedona Conference which is a standards body that has created specific guidelines regarding information governance and privacy. He noted that this Subcommittee is not swimming up against the stream. It is the direction things are going and the Nevada Supreme Court's action has acknowledged that.

Mr. Bates stated that things are moving fast, technology outpaces the law. There is an advantage to having people at this stage anticipate tech privacy issues and advise others.

Mr. Berghel asked Mr. Kandt about the mechanics of how to formalize the BDR process to create the Technical Privacy Subcommittee into a statutorily defined advisory board.

Mr. Kandt stated that he thought there were three things that would have to be flushed out in a bill:

1) Who sits on the advisory board;
2) How to define the scope of what the advisory board can study and make recommendations on; and
3) How to pay for the advisory board.

He advised the Subcommittee to send him any thoughts on the first two parts and he would share them with Assemblyman Bobzien. He has already given Mr. Bobzien a broad outline but did not address advisory board membership. Legislative attorneys will actually draft the bill.

The Subcommittee discussed alternative avenues for creating a stand-alone advisory board such as finding an existing public body more properly aligned with the work of the Subcommittee or creation of a new advisory board by executive order of the Governor. Mr. Kandt stated that there is no prohibition on the Subcommittee members for exploring other options, but to please let him know if anyone talked to a legislator other than Mr. Bobzien about it since Mr. Bobzien was already working on a BDR. It was noted that Mr. Bobzien's bill may be the best option since statutorily defined boards are more difficult to get rid of. Mr. Berghel stated that there are other legislators who are aware of, and supportive of, the work of the Subcommittee. It was suggested that the Subcommittee compile a list of interested legislators and share it with Assemblyman Bobzien so that he can rally support around it.

Mr. Kandt stated he was also monitoring BDRs to identify any potential bill that may be of interest to the Board or this Subcommittee.

Mr. Cobb asked if the recommendations of the Subcommittee were public information. Since both the Board and the Subcommittee are open meetings, any information presented is public.

5. Discussion and possible action on approval of May 30, 2014, meeting minutes.

Mr. Bates stated that he had sent Mr. Kandt some revisions to his remarks. Mr. Cobb made a motion to approve the minutes with his corrections. Mr. Bates seconded the motion. The minutes were unanimously approved.

6. Discussion with representatives of Nevada Institute for Autonomous Systems Unmanned Aircraft Systems (UAS) Program Management Office regarding Nevada UAS Test Site Privacy Policy (available at http://www.nias-uas.com/content/nevada-uas-test-site-privacy-policy).

Don Cunningham, the Business Operations Manager for Nevada Institute for Autonomous Systems Unmanned Aircraft Systems (UAS) Program Management Office, was in attendance. Mr. Cunningham was one of the original proponents for a UAS test site and was part of the team who wrote the response to the FAA's request for comment in the competition for Nevada to be designated as a test site. Upon designation, Mr. Cunningham went to work as the Business Operations Manager. He is also a test coordinator and speaks on behalf of the program to various interested parties.

Mr. Berghel stated that he had attended the first few UAS committee meetings when Ms. Laxalt chaired the committee. He faced resistance when he suggested that they take the time to develop a privacy policy so that they could direct the development if it were funded. Since he had never seen a clearly articulated privacy policy, he asked Mr. Kandt to arrange for Mr. Cunningham's appearance to talk about it.

Mr. Cunningham explained that he wrote the privacy policy and that there are several people in his office that handle interface with the privacy issue, but his office does not have a Chief Privacy Officer. He directed committee members to the website where the public can view the privacy policy (http://www.nias-uas.com/content/nevada-uas-test-site-privacy-policy). Copies were provided for the Subcommittee members.

Mr. Cunningham stated that the Test Site wants to get out in front, and try to solve some of the issues with privacy. He went over the highlights of the privacy policy. He said that 90% of the UAS missions will have no issues with privacy since they will be for research and development purposes carried out in areas with very little population. Currently, there are no projects involving surveillance products, although there might be in the future. They are looking to assist the FAA in integrating UAS into the national airspace system. Originally, the FTC was handed the privacy tag and it has now been moved to NTIA. The Test Site has briefed the FAA on eight white papers for research and development projects and one of those white papers was concerning privacy. They were instructed to then brief it to the FTC and NTIA. There is currently no funding, but they are looking for funding to get those projects engaged. Some are pure technological issues for UAS but there is also the privacy project on how to make the rules for unmanned systems. Unmanned systems follow the same law that currently in place for manned systems. Mr. Cunningham stated that he had learned a lot writing the privacy policy. Since the whole state of Nevada was declared the entity for the Test Site, he looked into Nevada law to look at policy for surveillance from the air. He was unable to find very much about it and so it comes back to privacy laws from the federal standpoint. Privacy is pretty well protected from a public entity, like the government or the police department. But the public does not have that same protection of privacy from a civil, commercial entity. When a civil entity does something that someone feels invades their privacy, they can be sued under tort law. The Test Site has requirements that are specifically written into the transaction agreement that the FAA has issued to each of the test sites, and those are pretty broad ranging. The biggest requirement was that the test site had to write and publish a privacy policy before they started flying. Nevada did this before being declared a test site. Some missions were flown in special use airspace, which was a restricted airspace with no population, and were not part of the FAA test site. The Nevada UAS policy procedure lists the documents reviewed by Mr. Cunningham to formulate the Nevada UAS Test Site's Policy. UAS evaluates each flight that they do in relation to privacy as they do the planning for it.

Mr. Berghel asked if anyone at the Nevada UAS Test Site was reaching out to the civil liberty groups to find out what potential issues might be.

Mr. Cunningham said that they were getting feedback through the FAA interface; interface with the other test sites, and by direct contact. He said they request comments regarding the privacy policy, which is posted on the website. Anyone can provide feedback and they are getting some. UAS also has a public outreach program to explain the program to legislators, city councils, and members of the public. Once a project is planned, they will anticipate potential privacy issues and will advertise to notify the public when there is a flight in the area. During the first year of operations, most of the flying is going to be small UAS that will flying be at less than 1000 feet, weighing less than 55 lbs., and flying pretty slowly. These will be the ones the public can easily see so Mr. Cunningham wants them to be especially aware that these operations will be taking place. There is also safety to consider, so they need to get the word out to the general aviation population, which will be sharing the sky, so that they can avoid each other.

Mr. Bates asked if anyone beyond Nevada UAS Test Site approved the posted privacy policy. Mr. Cunningham stated that the FAA does not have the authority to approve it. It is for UAS within the State or the Test Site to describe their policy. Beyond that, the FTIA would be the ones to look at it and they do not have a formal structure to approve a privacy policy. Any

information gathered by UAS will be reviewed by the Nevada UAS offices and, in the case of special use airspace, the offices of either DOD or DOE. Anything deemed unwarranted surveillance or that could be a possible privacy problem will be immediately deleted. Anything recorded for the purposes of research and development will be held for approximately 90 days. If there is a request to hold it for a longer period of time for the purposes law enforcement or a legal action, there must be a warrant in order to obtain the information.

Mr. Cunningham was asked who requires the privacy policy. He stated that the FAA required it for the test sites. After the test sites were designated, it was decided that because the FAA's responsibility is to handle the safety of the skies, not privacy, that responsibility has been given to the NTIA, which is the primary entity for the federal government handling privacy.

By Nevada UAS Test Site's own policy, the privacy policy must be reviewed annually and any changes made will be coordinated with NTIA. Mr. Cunningham hoped they will get a lot of feedback regarding the policy. Approximately every two weeks, there are meetings to discuss anything comes up in regards to their operations and so they are getting frequent legal advice, analysis and guidance from the FAA. Every six months, there is an interchange meeting with the FAA and all six test sites to discuss issues so they are getting a lot of guidance, but it was left to Nevada UAS Test Site to write their own privacy policy.

Mr. Bates responded to Mr. Cunningham's comments with two points:

1) There is a difference between manned and unmanned aircraft in terms of unmanned aircraft reducing the cost of surveillance so vastly; and

2) Various states have laws against paparazzi and that seems to be analogous to the kind of law that might apply to the private use of unmanned aircraft.

Mr. Cunningham stated that there is definitely a privacy piece to the issue. The test sites should not be problematic; it's more likely someone buying a DJI Phantom, which has a very capable camera, who might be a nuisance and create an intrusion of privacy. The Test Site has a public education campaign to educate the public on what the rules are, how unmanned aircraft can be used for good, and about safety issues. He noted that it is when you are intruding on someone's privacy that you are compromising someone's safety as well.

Mr. Bates asked if the NTIA sent some sort of approval for the privacy policy, or have they just not objected. Mr. Cunningham stated that they had not engaged yet.

Mr. Bates asked if the warrant requirement Mr. Cunningham had discussed was in the privacy policy or in writing. Mr. Cunningham directed the committee members to page 5 of the policy where it is written:

> Lacking definitive guidance by State of Nevada Statutes, the Nevada Test Site will comply with U.S. Federal laws and generally accepted privacy policy which prohibits using a UAS for surveillance to capture imagery of individuals or privately owned real property to possess, disclose, display or distribute for the purpose of legal action without a proper warrant. If

> operations at the Nevada UAS Test Site result in the unintentional capture of such imagery without proper warrant, the images will be destroyed.

Mr. Bates asked if there is there a structure that collects this data under the sole control of the test site. His understanding is that the test site provides a testing environment and support. Developers of UAS technology bring the equipment out there. He wanted to know who holds the data.

Mr. Cunningham responded that if you bring your system to the test site and you have a video stream coming back to the ground control station that is recorded (other than the situational awareness camera that is like a human eye that looks out front for flying) then the Test Site is required to review the images before they are released back to the developer. By contract, the record would be kept on file for review and the test site would take possession of the equipment for review. The data could be reviewed by any one, or all of three agencies looking at the surveillance before it is returned. It could be the Test Site as the PMO, DOD because of the proximity to the Nellis Test and Training Range, or the DOE. Anything recorded in surveillance mode is going to be reviewed by someone before it is released to be taken away in a digital form. They will also have a huge amount of empirical data from radar broadcast of the ADS-B, which is part of the FAA's air traffic management system. ADS-B is a location system that broadcasts the signals among the airplanes everyone can share their location and get other information. This data will be collected and used for research. For example, if there are specific tests to run airplanes and UAS in order to see if the algorithm works so that the aircraft can turn away from each other, there is going to be a huge amount of radar data. This kind of data will probably not be contentious. It's the EOIR and SAR sensor that can multispectrally locate someone's marijuana plants, for example, that will be problematic.

Mr. Bates asked if, once the agencies have cleared his data, he is allowed to sell it or do whatever he wants with it. Mr. Cunningham said, he supposed within reason, you could. The FAA has, within the OTA, and all agreements within the OTA, including contracts with customers, language within their contracts giving them certain data rights. If the information is proprietary, and the FAA has it, they can share it publicly. So there are a lot of checks and balances on who owns the data.

Mr. Bates pointed to the example of Google Earth and its mapping. There could be protests that come later on if you haven't decided on things ahead of time. It can become complex later on.

Mr. Cunningham stated that Google Earth might one day use UAV's for mapping, but that is several years away because the FAA is concerned about safety, and you may never see those in Las Vegas because of McCarran International Airport.

Mr. Elste observed that there are six different UAS test sites. He thinks there is a unique opportunity in Nevada because the privacy issues associated with UAVs and UASs is one of the most important aspects of the systems. If you can address the privacy implications of these systems at the same time you are developing the technologies, you can really move Nevada into the forefront of this industry. He wanted to encourage the Test Site not to

make privacy an afterthought and an inconvenience that has to be addressed by policy because its mandated, but to look at it as an opportunity to really excel in the industry.

With regard to the policy, he asked what the language "sensitive area" means. Mr. Cunningham said that these are locations which are classified or otherwise restricted airspace. Over 40 operating locations are being developed within the states. As they do that, they may find that there a spaces where members of the public declare they don't want UAS anywhere near them and they will take that into account as they plan their operations. They don't want to be a nuisance to people.

Mr. Cunningham was asked if, as part of the program, they would fly classified missions. Mr. Cunningham said that they may. Most of the operations are completely unclassified. They are looking to get integration of unmanned aircraft into the national airspace. At some point, they may collaborate with the Department of Defense because the Department of Defense has done a lot with UAS in a much shorter period of time than the commercial or civil sectors. There are operations that the Department of Defense would like to enable in the national airspace system as well, and there may come a time when they will collaborate together and some of those projects may be classified but they are not currently set up for classified operations.

Mr. Elste expressed concern that if they are flying classified operations, the ability to have transparency from a privacy perspective could be severely constrained. So the notion that the privacy policy protects all in all cases may not necessarily apply. The nature of the policy itself focuses specifically on adhering to the laws regarding privacy. It appears that the FAA OTA policy guidelines suggest that the policy should be formed by the fair information practice principles. He asked Mr. Cunningham to comment regarding to what extent he was writing the policy to the lowest bar –simply compliance with the law – versus writing a policy that actually incorporates fair information practice principles or the consumer privacy bill of rights. These policy items are not necessarily ensconced in law but are, in fact, considered to be common privacy practices and protections.

Mr. Cunningham stated that he had written the privacy policy with common sense in mind. He stated the privacy policy is a living document and that they are able to change it and repost it based on feedback or comments from anyone who feels there should be changes or additions to the policy.

Mr. Elste asked a question regarding disclosure of data to law enforcement if they have a warrant. He wanted to know if there is a similar constraint of disclosure of information to a private sector entity. Mr. Cunningham said that the data in all cases is covered under a confidentiality agreement and a non-disclosure agreement with the vendor they have. They are not allowed to release it unless the customer OKs the release to a private entity, so they have protection of their data. The Test Site has the ability to say no to anyone with the exception of law enforcement when they come with a warrant.

The devices can be used to collect a wide variety of data. The control of that data, and who is able to access that data is fundamental to the privacy concerns. It is not necessarily the collection of the data that is the primary concern; it's the housing and containment of that data once it has been collected. The privacy policy doesn't speak to the commercial

use of the data or other entities that are not law enforcement entities requesting or otherwise using the data. If platforms are collecting a variety of data, and the commercial entity that owns the data doesn't feel like it wants to destroy that data after 90 days as the policy requires, it seems to like they can share that information with whatever other party they are interested in sharing it with so it may not necessarily create a protection for non-law enforcement entities or for citizens from non-law enforcement entities.

Mr. Elste pointed out that the privacy policy states that "Neither the State of Nevada Constitution nor the State of Nevada's Revised Statutes have specific sections dealing with privacy that could be directly applied to UAS activity within the state." He thanked Mr. Cunningham for putting that into the policy and noted that that is the reason this body exists. It is important to address privacy as part of developing these technologies. If the privacy piece is done correctly, they can make sure this industry thrives.

Mr. Cunningham noted that 90% of the missions will have no privacy issues but they have to deal with everything-- from the size of a bumble bee to the size of a 737. It's a huge domain they have to deal with. It's truly something that will take work well beyond the end of the OTA for these test sites.

Mr. Victor thanked Mr. Cunningham on behalf of the committee and echoed Mr. Elste's comments on the importance of this program on the health of Nevada, the importance of program's privacy policy and how Nevada can be a leader in privacy issues, which could help establish Nevada as the go-to place for this industry.

He asked Mr. Cunningham if the feeds coming from current generation of UAVs use TCP/IP for their communication, or if he happened to know the protocol for communication between the human and the machine. Mr. Cunningham stated that most are not using TCIP/IP but can be immediately put into a TCP/IP environment. There are data wing signals which carry the data back to the ground control center, or another operating location, but they can be put into a TCP/IP environment. Initially the signals are coming in on an RF form. In most cases the feeds are not encrypted and that is one of the issues the test sites are working on. Mr. Victor said that there are significant resources available in Nevada to help do that.

Mr. Victor then asked if they had contemplated a non repudiable logging system which is a system that has its own tracking so that there is an audit trail to know that the policy is indeed being followed. Mr. Cunningham stated that they are not to that level of flying operations yet but those that they have had have been in the structured use airspace and they do have that type of log—one with the DOD and one with the DOE. They plan on keeping those types of logs and they need to do that in accordance with the FAA's rules.

Following up on an earlier question from Mr. Berghel, Mr. Victor asked if anyone at the test site was in communication with electronic civil liberty groups as they could be very helpful and provide guidance in this area. Mr. Victor said they had not and would like to be put in contact with them.

Mr. Victor also suggested that Mr. Cunningham open up the system and create an environment where researchers in security and privacy can examine and critique what they are doing in a laboratory environment. He stressed there are a lot of great resources in

Nevada that can assist the Test Site, such as a group called I am the Calvary that has researchers looking at unmanned, unaided systems called "The Internet of Things" and the security and privacy on those devices. More importantly, creating an environment for researchers would help make Nevada a leader in privacy and security.

In addition, Mr. Victor suggested that from a standards perspective, the separation of privacy and security and that role of responsibility be kept separate from other parallel roles so that there is reporting up the channel rather than laterally. Quite often in organizations, privacy and security is reporting to someone whose job it is to get something done on time and on budget, and so privacy and security gets pushed aside. It is important to have someone in charge of privacy and security on the same level and reporting up to someone who is then balancing the budget and time against privacy and security.

Mr. Cunningham said he would greatly appreciate the subcommittee's assistance in meeting with those individuals and groups that can assist in developing the privacy policy. None of the people working for the Test Site are privacy experts or legal experts so if the subcommittee can help point them towards resources, the Test Site will look to engage them and bring them in to help.

Mr. Victor then asked if they had contemplated a policy to deal with subpoenas. Mr. Cunningham said that the seven test site employees are support contractors for the Nevada Institute for Autonomous Systems, and they would look to them for guidance on how to proceed.

Mr. Cobb suggested that the test site contemplate how use of the information collected is handled. For example, a requirement to notify the test site if the information collected may be used for commercial purposes. Mr. Cunningham said that those kinds of requirements are included in the contracts of everyone they have worked with so far. There have not yet been any issues regarding retention of data or wanting to release the data to anyone else.

Mr. Bates noted that the hard part to predict is that there are companies who mash together disparate sources of data and combine them to determine a lot of things to very specific levels. Mr. Cunningham stated that the Test Site employees are cognizant of those types of possibilities and are watching for them. There is the possibility that data used for one purpose can show up in a different use case.

Mr. Berghel stated that he was not comforted knowing that they are using RF for their communication points. That is 30 year old technology and he thought they ought to be using TCP/IP technology. He encouraged Mr. Cunninhgam to take advantage of all of the people in the room who are innovating the security practices for TCP/IP. Getting open source solutions to the problem will give them a much better level of security. He hoped Mr. Cunningham would reach out to civil liberty attorneys and take the suggestions of the Subcommittee to heart.

Mr. Cunningham stated that he did want a robust privacy policy that ensures all of their operations are covered. What they have now is 15,000 copters with quality cameras on them shipped out by Amazon each month. You are not going to have to worry about the Test Site, it is the guys flying illegally every day within 5 miles of McCarran Airport, and over the

neighborhoods. The FAA does not have the resources to enforce all those instances of private misuse.

Mr. Berghel echoed Mr. Elste's sentiments in setting a leadership role for the State of Nevada in creating some legal constraints and accountability with regards to privacy.

The Subcommittee thanked Mr. Cunningham for speaking and told him he is welcome to stay involved by attending meetings.

7. Report from Allen Lichtenstein on project to identify all Nevada Revised Statutes that affect privacy rights. (Discussion only.) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

Mr. Lichtenstein was not present to give his report.

8. Report from James Elste on request for assistance from Electronic Frontier Foundation to develop legislation to expand online privacy rights. (Discussion only.) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

Mr. Elste stated he did not have anything to report. The results of the TCAB have not been shared either with the FF or any of the other parties they have been talking to. He was concerned that they may lose some of their enthusiasm for supporting the subcommittee's legislative efforts when there first fore fell flat. He hoped to be able to report to them that the subcommittee has made progress on other alternatives for supporting the work the subcommittee is doing.

Mr. Berghel suggested connecting them to the flight people. Mr. Elste said he was definitely going to spend some time talking to the UAS and get them connected to various resources.

9. Discussion and possible action on proposed amendment to the Nevada Constitution establishing a right to privacy.

The Subcommittee had nothing new to report regarding this item and no action was taken.

10. Discussion and possible action on proposed revisions to the State of Nevada Online Privacy Policy (http//nv.gov/privacy-policy/). (Discussion only.) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

The Subcommittee had nothing new to report regarding this item and no action was taken.

11. Discussion and possible action on proposed legislation to expand the news shield privilege under NRS 49.275 to address gaps created by technology.

The Subcommittee had nothing new to report regarding this item and no action was taken.

12. Discussion and possible action on proposed amendments to NRS 205.473-.513, *inclusive*, "Unlawful Acts Regarding Computers and Information Services."

Due to time constraints, Mr. Berghel skipped this item. It will be reorganized and presented for discussion in the future.

13. Discussion and possible action on request for Nevada Legislature to pass joint resolution calling on Nevada congressional delegation to expand online privacy rights under federal law.

The Subcommittee had nothing new to report regarding this item and no action was taken.

14. Discussion and possible action on possible revisions to the statutory definition of "personal information" in NRS 603A.040.

The Subcommittee had nothing new to report regarding this item and no action was taken.

15. Discussion and possible action on proposed legislation to prohibit Automatic License Plate Reader Systems in Nevada.

Mr. Berghel said that he did not like the way this issue was going in other states.

Mr. Bates said that at the last meeting, Mr. Lichtenstein raised the question of whether DMV information is public information – can you go to the DMV with license plate information and get owner information? The answer is no, with certain exceptions including consent, law enforcement, towing, insurance, private eye, employers of commercial drivers, car recalls, statistical studies, and the press.

Mr. Bates has been thinking about how it is possible to take a picture of a car as it goes by and look at the license number. Texas and Illinois have pretty good laws about biometric identifiers including faces and encoding. In order to do that you have to have written consent from the person and then there are time restrictions on destruction of that information and on further dissemination of that information. It seems to him that it's analogous to taking a picture of someone's license plate. In both cases you're saying its fine to take your picture in public; look at your picture and decide you are; send your picture to somebody else; but once you use technology to simplify or summarize it then it becomes something entirely different. Faces are a more private thing than a license plate, but if you are in your car they probably can't read your face and once you are out of your car they probably aren't reading you license plate. There is complementariness to it. As Justice Sotomayor said in the case involving GPS tracking, if someone knows where your car is, they know where you are – you might be going to a treatment center, a strip bar, an abused woman's shelter, any of that sort of information. In terms of tracking someone's cell phone, as far as he knows, private entities can't do that.

Mr. Elste said there are applications that can collect data from a cell phone that can be compiled into tracking information. MIT recently did an experiment where they loaded an app on a cell phone that didn't actually connect to wifi access points but recognized the SSID and was able to, within a matter of hours, not only track you but identify who you were. It's pretty powerful what can be done even if you don't have access to the phone's tracking data itself.

Mr. Berghel noted that IMSI-catching is available. The committee discussed the CIA tool, Stingray, developed by Honeywell. Most people to do not read the user agreements on the apps they download resulting in a significant number of people approving of being tracked when they put the apps on their phone. This speaks to a larger problem of ways this technology can be applied in ways that have adverse consequences. Once the met problem of tracking and the consequences of using this technology are understood, you can build frameworks for policy or legislation that define the context where that type of behavior is appropriate and warranted and useful and where it isn't.

Mr. Elste noted that license plate readers are a case of technology outstripping policy practices. People are doing this before anyone has really thought about the implications of it.

From a legal perspective the license plates are not specific identifiers. Neither are cell phones, but cell phones are more personal than license plates. License plates do not identify the driver though there is a strong correlation. Mr. Berghel asked Mr. Kandt if the Attorney General's office has an interest in the license plate issue. Mr. Kandt stated he could certainly discuss it with General Masto. Mr. Victor stated he had discussed the license plate data retention issue with Washoe County law enforcement about and they have an interest in reading license plates. He thought it would be prudent to talk to the AG. Mr. Kandt stated he would speak to her, however, she will be leaving the office in January and so her ability to pursue it will be limited.

Mr. Berghel asked the attorneys if they are of the opinion that the first amendment argument negates the point of Utah and Arkansas laws that the company has legitimate first amendment rights to protect.

Mr. Cobb stated that there was a plausible first amendment argument about dissemination of the information. Once they get it the information saying you can't communicate it to others, there is an argument there. The argument that the first amendment gives them the right to photograph and decode your license doesn't seem very plausible or persuasive. He stated that the politics of this will only get worse with time.

Mr. Elste said that he thinks there is a way to take this type of problem to look at collection and use of data and apply some broad techniques to address different types of things. The license plate reader is almost identical in terms of privacy and data handling as the UAS issue. There is very little difference in terms of the mechanics of collecting the information,

what you do with it, and what the downstream implications of it are. When we look at these problems and take the common elements like the reuse of data, we can apply the same sorts of principles to UAS, license plate readers, cell phones, etc. and really get to the heart of the matter. If someone collects a piece of data on you, without your consent, and its being used in a way that has some kind of consequence for you as an individual, it probably triggers a privacy concern which needs to be addressed. There should be some ways we can interweave some legitimate privacy concerns around that collection and dissemination of information.

Mr. Berghel requested that they subcommittee move directly to agenda item #19.

16. Discussion and possible action on proposed legislation to require full disclosure when metadata is captured and retained by government entities in Nevada.

There was no discussion or action taken on this item.

17. Discussion and possible action on proposed telematics black box legislation.

There was no discussion or action taken on this item.

18. Committee comments. (Discussion only.) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

There was no discussion or action taken on this item.

19. Discussion and possible action on time and location of next meeting.

Mr. Kandt stated he would check on availability for a meeting in October. The next meeting was subsequently scheduled for October 24, 2014 at 1:30 p.m.

20. Discussion and possible action on future agenda items.

Mr. Kandt stated that, with the Chairs permission, he would like to add 2 items to the next agenda. He would like to have a status update on the possible creation of a new, separate, technical or digital privacy advisory board. He would also like a discussion and possible action item regarding legislation that may be listed on the legislature's website. He will be tracking bills that may be relevant and will provide a report on that.

Mr. Elste would like an agenda item that would allow them to consolidate a series of discussion items that are privacy related. He thought it would be helpful to have an agenda item that would allow them to sort and prioritize the various privacy issues. Mr. Kandt will work with the chair and Mr. Elste to develop an appropriate description of this agenda item.

21. Public Comment. (Discussion Only.) Action may not be taken on any matter brought up under this agenda item until scheduled on an agenda for action at a later meeting.

There was no public comment.

22. Adjournment.

Mr. Berghel adjourned the meeting.