



April 2007

Dennis O. Williams

Editor

(comments to the editor at 254-8436 or denkare@aol.com)

THE PRIVATE INVESTIGATORS ASSOCIATION OF UTAH (PIAU) WAS SUCCESSFUL IN CHANGING THE LAW AND REMOVING THE DISADVANTAGES TO UTAH PRIVATE INVESTIGATORS

In 2003 the legislature passed legislation that required the Utah Bureau of Criminal Investigation (BCI) to issue private investigator licenses within five days after an application is received. The intent to have it applied to only apprentices didn't work and it spilled over to all applicants.

The change in the law opened the flood gates to allow persons from other states, whether licensed in their own states or not, to obtain quickie licenses in order to work in Utah and compete with private investigators living in Utah.

During the recent session of the Utah legislature the PIAU proposed changes to the law that basically returned the law to what it was prior to the 2003 legislation. PIAU members provided testimony demonstrating the unintended and detrimental effect of the 2003 legislation.

There are several positive things that have come out of this exercise. The 2003 legislation was meant to allow apprentices to obtain licenses within five days if they were going to work for agencies located in Utah. The PIAU has always recognized this to be a good thing.

The need for licensed apprentices by any given agency can be a rapidly changing thing. An agency might suddenly have a need for several apprentices and at the same time have several persons wanting to do the work but who are not licensed. Apprentices are required to be closely supervised by the agencies that employ them. Apprentices do not need to have any prior experience before becoming licensed. Consequently it placed an unnecessary burden on agencies to have to wait until the Utah Private Investigator Hearing and Licensure Board met every three months to issue new licenses.

The 2003 legislation solved this problem by allowing for apprentices to be licensed in five days and our industry is indebted to those who promoted that part of the legislation. However the 2003 legislation had more dire consequences which now have been corrected.

Of particular importance is that apprentices must work for agencies that are physically located in Utah and not for agencies located out of state. This was one of the big problems. What was to stop a person from another state from coming to Utah and getting a quickie apprentice license and claiming he is working for an agency in another state? The new legislation requires apprentices to work for agencies physically located in Utah.

The PIAU proposed reciprocity legislation this last session but it never was even heard in a legislative committee. One of the objections voiced to it was that it would give an unfair advantage to PIs from other states. This is not true. When we have leads in one of our cases in another state, that state is most likely to be one that adjoins Utah. Similarly if there was a PI who wanted to come to Utah to cover a lead that was part of his investigation, most likely he would be from a state adjoining Utah.

Idaho, Wyoming, and Colorado do not have state licensing for PIs. although some cities in those states may require local business licenses. These states can not take advantage of a Utah Reciprocity Law because they are not state licensed. Nevada, New Mexico and Arizona do have state licensing for PIs but none of them has reciprocity legislation in place. Personnel from the Arizona Department of Public Safety advised they recognize the need for reciprocity and they are in the process of promoting reciprocity legislation. Personnel from the New Mexico Private Investigator and Polygraph Board advised New Mexico has just passed reciprocity legislation but it will not be in effect for a year. So at present no PI from an adjoining state would gain anything if Utah were to pass reciprocity legislation. And Utah PIs cannot conduct any investigations in Nevada, New Mexico or Arizona unless they are licensed there as well.

The question is how we can get our own leads covered in another state where we may not be licensed. The answer is reciprocity in some cases. But Utah would have to first have passed reciprocity legislation for PIs. If a Utah PI were to conduct investigation in some states without a license from those states, he could be criminally prosecuted in that state and consequently lose his Utah license as well.

The reciprocity legislation proposed by the PIAU would require a PI from another state to first contact the BCI and explain what investigation he wanted to conduct in Utah and how long he needed. The legislation would only allow for leads to be covered and not for an investigation to be initiated in Utah. If he so chose, the BCI officer could then verbally authorize the PI from out of state to come to Utah for a specific number of days at the BCI's discretion, but not to exceed 10 days, beginning on a date specified by BCI. BCI would not be required to authorize anything. The out of state investigator would have to confirm this authorization in writing to BCI, so there would be an ongoing record of what out of state PIs were coming to Utah. The PI could not be subject to any discipline or criminal charges at the time of the request. The PI could not carry a firearm in Utah. Additionally, the PI must be from a state that has State Licensing.

We have much to gain and very little chance of losing anything if the reciprocity legislation is passed. No PI from an adjoining state would be able to come here unless his state passed reciprocity legislation as well. And there would be times when the reciprocity legislation would facilitate Utah PIs conducting investigations in more remote states. And since BCI would have a written record of PIs from other states that come here, this would be to our advantage as well.

Reciprocity is professional and we should all support it. Any concerns should be brought to the attention of the PIAU board of directors.

Dennis O. Williams has testified previously before the Utah legislature regarding these issues. He is a former President of the Private Investigator Association of Utah and served for four years on the Utah Private Investigator Hearing and Licensure Board. He is a retired Supervisory Special Agent of the Federal Bureau of Investigation.



**Observations of our Vice President
by Daniel D. Hooper
on Preserving Digital Evidence**

As investigators we are called upon to “investigate” a wide variety of offenses. We conduct surveillance, interview witnesses, read and write reports, and perform a multitude of other tasks related to our investigation. Most of us are fairly comfortable when confronted with most evidence we find while conducting an investigation. In some cases the evidence was collected prior to our involvement and we may only have to review what was collected. In other cases we may be the ones creating the evidence such as pictures or film during surveillance.

Recognize

So what do we do when we are confronted with digital evidence? You first have to recognize what digital evidence is. Any device that holds or stores digital media may be considered digital evidence and these devices come in a variety of sizes, shapes and colors.

Computers contain digital evidence. Computers can be categorized into three main areas: laptops, desktops, and servers. After the IBM PC was introduced in 1981 the number of computers in the United States has grown from 5.5 million in 1982 to over 260 million in 2006.

Cell phones contain digital evidence. Some law enforcement labs have entire units dedicated to the forensic analysis of cell phones. There were 200 million cell phone subscribers in the United States in 2006. The distinction between cell phones and PDAs is becoming blurry with more and more cell phones and PDAs being combined into one unit. Cell phones and PDA both frequently contain cameras and have the ability to store extra data on flash memory cards. Some PDAs are the equivalent of a small computer with a windows based operating system and the ability to run a variety of Microsoft programs such as Word and Exel.

Thumb drives or USB devices contain digital evidence. These devices are small, inexpensive and make take a variety of shapes. There are thumb drives enclosed in watches, glasses, pens and Swiss Army knives and have also been disguised as rubber ducks, Barbie Dolls, sushi and shrimp.

Flash memory contains digital evidence. Flash memory is used in cameras, cell phones and PDAs. The most common types of flash memory are CompactFlash, Secure Digital (SD), Memory Stick and XD cards. There are several variations of SD cards and Memory sticks.

The primary storage device in a computer is the hard drive and these come in a variety of sizes and flavors. The most common size of hard drive for desktop computers and servers is

3.5" while the most common size of hard drive for laptop computers is 2.5", but hard drives may also be found in 1.8" and 5.25" sizes.

Plan

The first step in preserving digital evidence is to plan Who, What, Why and Where.

Who is the user and what do we know about them? What are the user's computer skills? Is the user a novice user or an experienced computer programmer? Is the user paranoid? This will help you get a picture of what the user may or may not do or be capable of doing. A paranoid user with strong computer skills will be more likely to have strong passwords, encrypted files and hidden or disguised storage media.

What kind of digital evidence? What type of operating system? Is the computer a Windows based system or is it Apple or Unix based? The type of system will determine how you handle to the evidence and who is qualified to examine it.

Why are we taking or looking at the system? Do we have the proper legal authority? If the case is administrative, are the proper policies and procedures in place to allow you to look at it.

Where is the data stored? Data can be backed up or stored in variety of ways. Tape backup was the most common method of backup, but there are offsite backup storage facilities, online backup and stand alone storage systems attached to a network (NAS). I have been involved in a search where after the search warrant was served it found that all of the data we were looking for was stored at an off-site facility in a different state.

Involve a forensic computer expert as soon as possible.

Protect

Unlike the popular CSI shows, handling digital evidence requires some thought and the first step should not be to turn on the computer and start looking around. The first three rules of computer seizure are "Don't touch the computer", "Don't touch the computer" and "Don't touch the computer". Digital evidence is fragile and can be easily changed.

Move people away from the computers. Check the computers for phone lines or network connections. Look at the screen and see what is running. Document, document and document. In 1994 when I first started handling digital evidence the next rule was fairly clear. Pull the plug to shut the system down. Now days things are not that simple.

What if you look at the screen and see an important document that is open. If you pull the plug and the document has not been saved and the timed backup has not run or has been turned off, you will lose that document. The same thing applies if you disconnect the network cable and the document was being stored somewhere else on the network.

If the user has turned on encryption (EFS) on an NTFS file system and you shut down the computer, you will not be able to access any of these files with the user's password. If the user has an encrypted document open you will not be able to open the document again without the password. Once again, unlike CSI, good encryption programs are very difficult if not impossible to break. A 128-bit key has 339,000,000,000,000,000,000,000,000,000,000 different combinations. Even if you had 10,000 computers checking a 1000 keys per second, it would take... Well, you do the math, it would be a really, really, really long time.

Do you shut the system down or image the system live. What are the advantages and disadvantages of both methods? If you shut the system down you may lose valuable evidence, but you protect the system from any further changes. If you image a live system you may gain some valuable evidence, but you will make changes to the system. What you do depends upon what you have learned about the user and the type of system and software they use.

Create a forensic image. Regardless of how you have handled the evidence so far, you need to make a forensic image. There are several programs available on the market to do this and the most popular format is an encase image or E01 and a dd image or raw image. The most popular tools for creating these images are Encase (Guidance Software) and FTK Imager (Access Data Corp). Once your forensic image is created check that image against the original to verify that they are the same. This is usually done by creating a hash value or mathematical fingerprint of the data and comparing it. This can be done with both Encase and FTK Imager and the hash value of the imaged device is stored with an E01 file when it is created.

Once you have created your forensic image, make a backup. Hard drives fail. This is not always possible or practical, but speaking from experience, hard drives fail and when they do, you have lost all of your evidence.

Transportation and Storage

Use care when transporting computers and digital evidence. If you drop it, it will probably break. Don't use non static plastic bags to store computer related evidence. Magnetic media can be altered by magnetic fields. Store your evidence in a clean, dry and cool environment. Cell phones and PDAs must be turned off and stored on chargers. The typical battery life is usually no more than 30 days.

Examination

Last but not least use a trained and experienced examiner. A computer expert does not always equate to a forensic computer expert. Don't be afraid to ask questions and check credentials.



Officers

President

Mel B. Ashton
(801) 553-0774

Vice President

Daniel D. Hooper
(801) 250-4450

Secretary

Kimberly K. Cooper
(801) 688-3215

Treasurer

Kris Cantil
(801) 298-0940

Board of Directors

Chairman

Van Canann
(801) 465-9007

Members

Jake Allred
(801) 404-1666

Mike Barker
(801) 280-1647

Veronica Hitt
(801) 563-3377

Doug Huntsman
(801) 798-0635

Kevin Johnson
(435) 224-5388

Dennis Williams
(801) 254-8436

To contact PIAU members, first go to piau.com, then select members. Those with agency licenses are listed first. Then those with registrant and apprentice licenses are listed.



The Private Investigators Association of Utah (PIAU), is doing quite well and our membership is high. So far, I have heard that most agencies are doing well; however, some apprentices have had to return to former employment to make ends meet. The investigative jobs weren't coming as often as needed to keep their bills paid.

I feel badly that this has happened because we have need for good private investigators in Utah and an apprentice is where it all began for many that have agencies today. I hope that we will have sufficient work to keep those who really want to be private investigators in the business.

We are well into the first half of 2007 and we fared pretty well in the Utah Legislature and not so well in the US Legislature. First the Private Investigator Regulation Act was amended. In 2003, the law was changed to allow licensing of private investigators within 5 days This didn't give ample time for a background check on applicants.

The intent of the law was to only allow apprentice investigators to obtain a license within five days; however, the Department of Public Safety followed the law to the Tee and was licensing any applicant within five days that didn't show up on a BCI check.

This also created the problem for us with out of state agencies coming to Utah, getting a license and working cases in Utah and taking the profits back out of state. Also, some of the major investigative agencies were having individuals get an apprentice license and then they would assign them cases to work in Utah.

This did not meet with the intent of the law that says that an apprentice must work under the close supervision of an agency. You can not be in another state and closely supervise an apprentice. If the apprentice needs help, the telephone may not be close enough. SB 254 was drafted by John Tinsley and Mel Ashton and sponsored by Senator Margaret Dayton. Both John and I testified on behalf of this bill at the Senate Committee and it passed with a unanimous vote.

It cleared the Senate with a unanimous vote. On the last day of the legislature, the bill was sent to the House as a Senate priority bill by Senator Dayton. We contacted all of the House leaders and solicited their help in passing this bill. It was passed around 9:30 p.m. and the Senate President signed the bill. On March 14, 2007, the Governor signed the bill into law.

What this means is that only an apprentice can get a temporary license within five days. Then the apprentice must work only for a private investigative agency licensed and located in Utah.

We didn't get the Reciprocity Legislation passed. Our sponsor in the Senate let the bill set there and die. We will try to get a different sponsor and try to get the bill passed in the 2007/2008 Legislature.

We also put forth a Process Service bill that would exclude the 18 and not a party to the action. The bill failed because there was not schooling in place to let those in that category become educated before serving process. We are looking into possible solutions to having more professional process service performed in Utah.

At the Federal level we took a hit with HR 4709, "Telephone Records and Privacy Act of 2006." Many of us used telephone toll information for legitimate investigative purposes. A few years ago, I was able to recover a kidnapped child using telephone toll information.

Unfortunately, many internet sites offered these services to anyone with \$125.00. They even sold the FBI their undercover telephone tolls. Then there was the Hewlett-Packard case we all saw in the papers. It happened in California and California had a law that applied to the obtaining of telephone tolls. There were indicted PI's and officers in HP. All of this publicity incited the US Congress and subsequently the mood was set at tightening up information sources.

The law that passed prohibits the sale and transfer of confidential phone records without prior authorization from the customer. NCISS supported this bill in Congress because of the mood existing there.

There are two other bills dealing with privacy: S238, the Social Security Number Misuse Protection Act; and S329, the Notification of Risk to Personal Data Act of 2007. Should we loose access to Social Security Numbers and Dates of Birth, our work would be much tougher.

I wish each of you a prosperous 2007 and hope that each of us stays healthy and happy.

Mel Ashton
President, PIAU

**Welcome New PIAU Members
By Kimberly K. Cooper
PIAU Secretary**

The members of the PIAU would like to welcome all of the following as new members of the PIAU:

Erin Uribe
Georgia Canann
Rusty Richards



From the desk of the:

Chairman of the Board



How We Charge Into Danger, Matters

Years ago, a lifetime ago, while directing traffic in Detroit around a fire scene, one wall of a burning building fell toward a fireman. He had just taken his metal ladder down from that very place and was walking away. As I ran toward the giant dust cloud that hid him from view, the dust began to clear and I was relieved to see he was still standing and uninjured while holding one end of his now crushed ladder.

As I walked back to my duty in the street, my mind was filled with this and dozens of other memories. Why did I instantly charge into the unknown dust and smoke? Or recently chase a diabolical doer of dark deeds down a darkened alley, or join in high speed pursuits, or become involved in undercover life with truly evil bad guys? In all these situations, good sense would suggest running away would be the wiser action.

We work in a business, not unlike soldiers, firemen and policemen. We charge at difficult times into places to help others by doing things and dealing with people that our clients would rather not. Thus, our great value!

But working often times on the edge of danger and evil, entices some investigators across the country to overstep the boundary of professionalism, ethics and legality. Movies and television make this type of person seem to be a hero and the norm. Of course, this is not true.

We are living proof, in the PIAU, that men and women of good judgment and character can perform quality assignments for our clients and not cross over to where the bad guys spend their lives, while at the same time we step into peril and the unknown.

**HOW TO JOIN THE PRIVATE
INVESTIGATORS
ASSOCIATION OF UTAH**

To join the PIAU or to contact any of our members, please go to our website at PIAU.COM and follow the instructions to print out an application.