INTELLENET QUARTERLY

JUNE 2011

TABLE OF CONTENTS

Carino's Corner

James P. Carino, CPP, VSM
Executive Director

The 28th Intellenet Conference, held at the Double Tree Hotel in Crystal City Virginia (Washington, DC) 13-16 April 2011, was by all indications a smashing success. Old timers welcomed in many first time attendees and the Auction raised almost $7,500 in support of the Philadelphia VA Palliative Care. It was our second highest attended conference with over 120 attending all or part thereof. My personal thanks to our local host, Nicole Bocra, to Robert Dudash who put together another outstanding speaker program and Nancy Poss-Hatchl for organizing the great auction. We also had the pleasure of Graham Dooley and Cathy Castorani debuting as Auctioneers, as well as our behind the scenes crew peddling the 50-50 raffle tickets as an additional fund raiser.

Honored at the Saturday night Gala was Geoffrey Hughes (UK) who received the Lifetime Achievement Award, acknowledged for his many years of dedication and commitment to Intellenet. A major highlight of the Conference was our Thursday lunch speaker, six time Pulitzer Prize winner Jeff Leen of the Washington Post. Jeff also joined us at the two dinners.

Our Hospitality Suite, open all four nights, drew not only a big output of war stories but also served as a "recruitment" for a few new special initiatives. These will forever remain publicly unannounced as to details but join our three already in progress. These initiatives

are in keeping with a primary goal to increase billable time for our members by promulgating our capabilities to perform investigations for national and international clients. In addition to these already "on the books", I note that as of this writing at least three more initiatives are in advanced discussion stages and look encouraging for developing into "done deals" within the next 30-60 days. Concomitant with these initiatives is targeted recruitment of new members to increase both domestic and international coverage.

Our next Conference scheduled for Vancouver Canada 16-20 May 2012 is also almost fully planned with the speaker program pretty set. Our venue hotel is the Westin Bayshore. Our local host, Kevin Ripa, has lined up a great hotel rate including many extras and is now planning the "networking" opportunities. Our Travel Agent guru Suzanne Drumm is also exploring both cruises and the Great Canadian Rail Tour venues for those desiring pre or post Conference touring throughout Canada and Alaska.

Know Your Fellow Member

Eric Douglas De Van was born and raised in Philadelphia and graduated with a BS in Criminal Justice from West Chester University. He was nominated as a Distinguished Graduate of the Criminal Justice Program. Mr. De Van began his career working undercover investigations in the power, communication, jewelry, and cellular phone industries. Investigations included: theft, murder for hire, child pornography, drug, and gun running.

After moving to Columbia, SC in 1996, De Van & Associates Security Consulting was formed. Eric De Van was named the 2003 South Carolina Governor's Office Small Business Success Story as well as being named the Small Business Ambassador to the City of Columbia in Canada. He has worked with the US Department of Commerce on security trade missions in the Dominican Republic.

Besides Arson Detection training with the Philadelphia Fire Department, Eric De Van was a Death Scene Investigator as a Deputy with the Richland County Coroner's Office. Although Mr. De Van provided executive protection and has defensive driver trainer with the South Carolina Law Enforcement Division and conceal carry permit, he installs high tech surveillance equipment in prison facilities, post offices, day care centers, and open air parks, the focus of De Van & Associates is pre-employment screening and drug testing for universities and municipalities.

Members in the News

Jay Groob, American Investigative Services, Inc. Brookline, Massachusetts was a Panelist along with two Massachusetts Justices of the Probate and Family and an attorney on the topic of "Discovery in the Electronic Age". **Barry RYAN** (PA) has been elected to the Board of Directors at the University of Notre Dame. **Susan CARLSON** (IL), **Jim SILVANIA** (OH) and **Michael WEST** (AR) all have feature articles in the April 2011 issue of "PI Magazine". Also appearing is **Michele STUART's** (AZ) monthly column titled "Internet FYI. The feature in a series of stories, titled "Profile of the American Woman PI" highlighted Intellenet members (in order of appearance) **Lynn LEVY** (MD), **Pat SHAUGNESSY** (AZ), **Nancy POSS-HATCHL,** (CA), **Lynda BERGH** (CA), **Susan LAJOIE** (wife of John-MA), **Nancy BA**RBER (CA), and **Joan BEACH** (VA). Full page write-ups with photos highlighted **Linda MONTGOMERY** (WA),**Jayne McELFRESH** (AZ), and **Kitty HAILEY** (PA), **Al Ristuccia,** (CA) is a speaker and **Cynthia Herrington**, (NJ) is a Presentation Moderator at the IAAR Conference in London, June 12-14, 2011; **Brian Ingram** (TX), **Jimmie Mesis** (NJ), and **Gary Kuty** (OH), presented at the Associations One Conference May12-14 in Dayton, OH; **Steve Rambam,** Brooklyn, NY conducted a 3 hour seminar on April 14 at the Society of Investigators of Greater Newark; **Nicole Bocra**, Arlington, VA presented at the North Carolina PI Association in Ashville, NC; **Barry Horvick**, Alexandria, VA was a speaker at the 5th Life Settlement and Longevity Conference in New York City on April 28; **Harriet Gold**, Norcross, GA was a presenter at the South Carolina PI Association seminar on May 5-7 in Myrtle Beach, SC; **Phil Curlewis**, Hong Kong, and **Meyer Nudell**, North Hollywood, CA were presenters at the Protective Security Conference June 8-9 in Baltimore, MD; **Bill Blake**, Littleton, CO was a presenter at the NCISS Annual Conference April 29 in Vail, CO;

New Members

Dave Keylon, Key Investigations, Albuquerque, New Mexico; **Gard Westbye**, O.P.E., Oslo, Norway, **Robert Dower**, Dower and Associates, San Francisco, California,

NEW TECHNOLOGIES OFFER NEW OPPORTUNITIES FOR FRAUD

Bill Marshall
Vertis Intelligence
Fairfax, Virginia

Never let it be said that criminals do not stay on top of the latest technological advances in furtherance of their business.

In 2010, we investigated a suspicious death claim involving an individual who was insured for many millions of dollars through multiple insurance companies. After an extensive investigation, we concluded with a high degree of certainty that the claim was fraudulent. The insurance claim was fascinating from an investigator's perspective, because the perpetrator was very clever and clearly understood the nuances of the insurance business. The fraudster knew how long to wait before filing the claim in order to minimize the amount of investigation conducted, which documents would be of most importance to the insurance companies for payment of the claim, and even the kind of beneficiary that would raise the least suspicion on the part of the insurance companies. Perhaps the most intriguing aspect of the case was the use by the perpetrator of a fairly new database created by a division of the US Department of Justice to further his scheme.

We will not go into great detail of the case in this article, as it is currently under criminal investigation, but the case illustrates a potentially new tool for use by criminals. The heart of the fraud involved the creation of a fictitious insured by the perpetrator of the scheme. After creating a person out of whole cloth, and insuring that fictitious insured with many insurance policies, the perpetrator decided the time had come to "kill off" the insured and file claims for the death benefits. The major obstacle the perpetrator faced was producing an actual physical body that could be used as the "insured" and have the requisite death certificate produced for presentation to the insurance companies.

The perpetrator in this scheme solved this problem by turning to a database available via the Internet that was established in recent years by the Office of Justice Programs, a division of the US Justice Department. The website, called namus.gov, that houses the database is accessible to the general public and bills itself as a clearinghouse for records of unidentified bodies that have been discovered across the United States. Medical examiners from around the country can enter photographs and descriptions of unidentified deceased individuals whom they have autopsied, along with descriptive information regarding the location where the bodies were found, clothing they were wearing, gender, approximate age, race and other identifying information. Dental record information of the decedent may also be included. The name of the medical examiner and his or her agency are also listed. Each body is assigned a case number and a case manager within the program to whom inquiries can be directed.

Such a clearinghouse in concept can be a very useful tool for medical examiners and law enforcement officials, as well as members of the general public who are searching for missing relatives. It can bring together those who have evidence with those who are searching for answers, and do so in a very inexpensive and efficient manner. The ability to photograph unclaimed/unidentified bodies, and post those images, along with descriptive information, virtually instantaneously on a globally accessible website is a potentially great technology for solving crimes and helping people find missing loved ones.

Unfortunately, like any new technology, it has also been used for nefarious purposes. In the case of our fictitious insured, the perpetrator of the scam used the database to locate a body that he claimed was the insured. The body had enough similarity to the fictitious identifying information contained about the insured in the insurance applications to be acceptable as the "insured." The gender, approximate age, and ethnicity of the body were fairly close to the bogus insured.

The perpetrator of the scheme then contacted the medical examiner who was identified in the database as having autopsied the deceased and convinced the medical examiner it was the insured. The medical examiner, not suspecting anything untoward, then issued an

official death certificate in the name of the insured individual which the perpetrator, acting as the claimant, used to submit to the insurance companies which had issued the policies. Once the insurance companies had the death certificate in hand, listing the fictitious insured's name, they had sufficient proof-of-death to pay the death benefits. The perpetrator had waited to "kill off" the insured just past the policies' two year contestable periods, thereby limiting the amount of investigation the insurance companies could undertake as part of their claim validation process.

Although millions of dollars were initially paid on some of the fraudulent claims in this case, our investigation revealed the scheme in sufficient time to allow us to track down and notify all of the insurance companies that had issued policies on the fictitious individual. The insurance companies which had paid their claims were able to freeze the funds for the most part, and only about $1 million in pay-outs were not recovered. As of this writing, the perpetrator is being sought and efforts are being made to apprehend and prosecute him.

We would note that the suspected perpetrator in this case, whom we had investigated in an earlier life insurance scam, was a fairly sophisticated white collar criminal who knew the workings of the insurance business. Fortunately, most insurance fraud perpetrators do not have as much savvy. The use of the unidentified bodies database by this criminal was a novel and intriguing aspect of this case, in our experience.

While we have simplified the description of the case above for brevity's sake and to preserve the integrity of an ongoing investigation, there were many indicators of fraud that appeared during the course of our investigation, though most of them were subtle. Improved due diligence prior to the issuance of the insurance policies by, for example, verifying the claimed income and stated employment of the fictitious insured, could have averted the insurance policies from being approved. At claim, a notable lack of information provided by the claimant as to the exact cause and manner of the insured's death was a telltale indicator of fraud in the case as well. But the use of the Justice Department's handy new unclaimed bodies database was perhaps the most instructive element of the case.

Insurance fraud perpetrators will likely continue to exploit such new technologies and include them in their schemes. Savvier criminals will also exploit known vulnerabilities in traditional insurance claim processes. Once again, vigilance at all stages of life insurance transactions – from sale of the product through claim verification – is necessary to limit the occurrence of fraud.

Book Reviews

Jeff Leen
Investigations Manager
Washington (DC) Post Newspaper

Basic Private Investigation

A valuable primer that covers all the bases of the private investigation business, from setting up a firm to marketing and professional ethics. It also offers a comprehensive overview to the skills needed to make such a business successful, with incisive tips on interviewing, working in the courts and surveillance. The chapter on how to write a professional report alone is worth the cover price. An essential guide for anyone making the transition from law enforcement or military to private sector investigations.

Advanced Private Investigation

A deep dive into private investigation, distilled from the minds of battle-tested practitioners. This is truly an advanced course that will enhance any investigator's repertoire, regardless of background.
Goes beyond the nuts and bolts into the thinking behind the mechanics that will allow you to raise your investigative game. Full of pearls of wisdom laid out with wit and grace, like this one: "For instance, just because a person is noted for having presented on a regular basis at seminars does not mean he or she actually has any practical ability in 'the field;' talking heads generally have no corpus."

What I Learned From Editing the Intellenet Books

Bill Blake
Blake and Associates, Inc.
Littleton, Colorado

Disclaimer: I am not an English teacher, did not major (or minor) in English while in college and would starve to death if I had to make a living as a writer of anything short of obscene notes to good looking women!

While in high school, I had a very cavalier attitude toward studying; particularly those subjects, aka English, which did not interest me. My original goal in life was to be the baddest cop in my hometown. Considering the political atmosphere at the time, the town fathers provided everything I would need to be a cop—gun, badge, bigger than real club, and a car that worked about two hours a week. What a life to look forward to!

When I started my first year of high school, my attitude was forcibly changed for me by a lady who I really learned to admire over the years. Miss Ann Hennessey was the Freshman English teacher and there was only one way English was to be learned—HER WAY. Not that she had been around a while but one of the first things she told me was that I was a spitting image of my father who had been one of her students. Like father, like son, I was as dumb as dirt when it came to English and she was going to change that if it killed ME. That was in the days when corporal punishment, aka the teacher, was a common part of school life, and with her sometime not too subtle assistance, I must have accomplished something—they allowed me to graduate from high school or was it that they didn't want me to stay around any longer?

Reading the various chapters that were submitted for inclusion in one of the two books, I learned many things: (1) The professional knowledge of the Intellenet members is unbelievable. (2) Not everyone was an English major in college. (3) After working with the publisher's editorial staff, I realized that I needed a refresher course in English grammar. To remedy my lack of English grammar skills, I contacted several sources: My middle- and high school neighbors; the library; the internet and my document reviewer—my wife. One particularly appropriate publication was *Grammar Essentials for Dummies* by Geraldine Woods and published by Wiley Publishing, Inc. which became an English Bible for me.

For my benefit, I put together the following cheat sheet which is still beside my computer even though the books are now available to the public.

HE/SHE: You should say *he* or *she* and *his* and *hers* when grammar requires such terms. The masculine or feminine universal may be offensive to some people.

COMMAS: You need commas between each item on a list, with one exception. The comma in front of the word *and* is usually optional because when you say *and*, you have separated the last two items. Don't separate numbers from other descriptions or from the word(s) they describe. The pronouns *which* and *that* help decide whether you need commas. *That* generally introduces information that the sentence can't do without—essential information that you don't set off with commas. The pronoun *which* often introduces nonessential information that may be surrounded by commas. At the beginning of a sentence, a phrase that starts with *because* acts as an introductory remark and is always set off by a comma.

WHO/WHOM: You use *who* and *whoever* as subjects and to complete the meaning of linking verbs. You use *whom* and *whomever* for all kinds of objects.

This is just a very short list of the major things I had to relearn. Am I a better writer? I'm not sure but it was a great reeducation for me. Miss Hennessy would be proud of me just for making the effort but her original opinion of my skills probably won't be dramatically affected—I'm still as dumb as dirt when it comes to English Grammar.

Court Ruling Deals Blow To Insurance Companies Over Stoli Policies

Bill Marshall
Veritas Intelligence
Fairfax, Virginia

Stranger originated life insurance (or "STOLI") policies have long been a controversial financial vehicle, and a November 2010 ruling in New York's Court of Appeals is likely to perpetuate the controversy.

STOLI policies are life insurance policies that are usually issued to well-heeled, elderly individuals who sell the policies to unrelated investors (i.e., "strangers") shortly after they are issued. They are applied for with the intention of selling them to a stranger and are expressly used as a speculative investment by unrelated parties (as opposed to life settlement transactions, in which a life insurance policy is taken out for traditional insurances purposes, but is later sold by the owner to meet unanticipated immediate financial needs.) STOLI policies became popular in recent years among investment firms, who pay the premiums on the policies and receive the death benefit following the insured's demise.

In a typical STOLI transaction, a STOLI promoter contacts a prospective insured – generally a person of advanced age and some affluence. The promoter offers the individual "free" life insurance for two years (that is, the contestable period of the insurance policy), in which the promoter offers to pay the premiums for a policy (usually with a sizeable face amount of $5 million or more), and often includes an added inducement, such as the gift of a new car to the elderly person, or a vacation, or cash. There are variations on how the insurance premiums are paid. In some cases, the promoter pays the premiums directly. In others, the insured pays the premium with a non-recourse loan from the promoter, with the insurance policy being used as collateral. If the insured walks away from the loan, the promoter takes

possession of the policy. If the insured elects to keep the policy at the end of the two-year contestable period, he must repay the promoter the loan principal, plus interest. In either case, the insured himself does not fund the policy.

After the initial two-year period, when the promoter assumes ownership of the policy, he will generally resell it to other investors. These schemes often entail additional facets. In some cases, the insured is offered a small percentage of the death benefit for his family upon his death (such as $1 million from a $5 million policy). In many cases, the promoter will establish a charitable trust. Investors then purchase bonds, with the proceeds funneled into the trust. The trust funds are then used to purchase single-premium life annuities on the life of the insured and the annuity payments are used to purchase large life insurance policies on the insured (and give an immediate return on investment to the investors). When the insured dies, the investors then recoup their investment, receiving the lion's share of the life insurance policy's payout, with a small amount of the death benefit (typically five to seven percent) going to the charity for which the trust was established.

In any variation of the above scheme, the primary goal, and the source of the controversy over the use of such policies, is to allow investors to make a profit from the death of a person to whom they are not related and in whose life they have no interest.

Insurance companies, who potentially are exposed to huge liability as these policies mature over the next 10 years (estimated by some to be as much as $100 billion[1]), argue that the concept behind the STOLI policy violates 300 years of established British and U.S. "insurable interest" laws and social policy, which dictate that only a person with a personal stake in the continued life of another (i.e., an "insurable interest") should be permitted to benefit from a life insurance policy on that individual. STOLI policies, much like the "dead pools" of old England in which Britons would wager on the date of death of British nobility, are wagers on the life of another. Insurance companies have filed dozens of lawsuits across the United States challenging the validity of STOLI policies.

The court ruling in New York may severely hurt the insurance industry's legal challenges to these policies. In the New York case, a wealthy attorney, Arthur Kramer, had taken out $56 million in insurance policies and then immediately sold them to hedge fund investors. When Mr. Kramer died in 2008, his widow sued for the insurance proceeds, arguing that the transactions with the hedge funds violated New York's insurable interest laws and the benefits from the life insurance should go to Mr. Kramer's estate. Two of the insurance companies which had issued Mr. Kramer's policies also sued, arguing that neither the hedge funds nor Mrs. Kramer should receive the death benefits, because the insurance policies were illegal from their inception.

Insurance companies around the country followed the lawsuit closely, given the multi-billion impact an unfavorable ruling would have on their industry. The court ruled in a 5-2 decision in favor of the hedge fund owners of Mr. Kramer's insurance policies. The court found that a person has the right to take out a life insurance policy on himself for the purpose of selling it to another, without violating the state's insurable interest laws. Such transactions, the court found, in which a person knowingly takes a life insurance policy on himself and sells it to another does not constitute a wager on that person's life.

[1] Figure cited by California State Senator Mike Machado in KCRA 3 News report, "Investors Could Profit from Strangers' Deaths." January 31, 2008. Available at http://www.kcra.com/r/15189803/detail.html.

The court's ruling is likely to impact ongoing litigation by insurance companies across the nation. An attorney for the hedge funds, Julius Rousseau, said, "I think Kramer will go far beyond the borders of New York and will be a very important case in settling the industry and ultimately giving greater certainty to investors that they can buy" life insurance policies without fear of insurers or heirs contesting their legality.[2]

The major insurance industry associations, such as the American Council of Life Insurers, have pushed for changes to state insurance laws to eliminate STOLI policies, and many insurance companies will not knowingly issue such policies. Twenty-eight states, including New York, have passed laws in the wake of pressure from insurance companies to restrict the ability of people to sell their life insurance policies. Many companies' life insurance applications now ask an applicant if he intends to sell the policy. (The implications of such language in a policy application may itself be tested in court challenges one day.)

In our experience, STOLI policies also tend to show a higher incidence of misrepresentation at application regarding the insured's true medical history and net worth, as the promoters of the policies seek to obtain the highest possible face amounts for the policies of elderly individuals. In light of the ruling in Kramer, it will be in the interest of insurance companies to increase their vigilance of policies that fit the profile of STOLI, and to conduct very thorough due diligence of insurance applicants before the issuance of high-dollar policies.

ACCEPTABLE USE POLICIES

Kevin Ripa, EnCE, CDRP, CEH
Computer Evidence Recovery, Inc.
Calgary, Alberta, Canada

In today's business world, computers are as ubiquitous as the pencil and paper of yesteryear. Most any type of business cannot function today without the use of computers in one fashion or another. It seems a paradox, then, that at no other time in history has the commodity of time been stolen and wasted by employees as much as today. These computers that were supposed to speed up our tasks and make us so much more efficient are being used as tools with which to waste more time than we could have ever been able to without them.

Imagine finding out that an employee has been wasting as much as 1-2 hours per day using the computer to surf the Internet or chat online with friends. As a supervisor, you let them know that their services are no longer required for obvious reasons. Mere days later, you are served with a Statement of Claim for wrongful dismissal. The claim? Nobody ever told this employee that they couldn't perform such activities. This has been used successfully in the past. This sadly is the unfortunate byproduct of a legal system in a severely litigious society.

In order to respond to this type of travesty, we meet the challenge with a Corporate Acceptable Use Policy (AUP). Every company or entity with more than 1 employee (the owner) should have a strong AUP in place, and yet easily less than 40% of businesses have them. Most small businesses would say they aren't big enough to need one, but our example above shows that even 1 or 2 staff members could cause problems such as this. Even worse, the smaller your company, the larger the impact from a frivolous lawsuit.

[2] Maremont, Mark and Leslie Scism. *The Wall Street Journal*. "Ruling Gives Life to Death-Bet Insurance." November 18, 2010.

There should be no question that an AUP is a necessary and integral part of any business's computing environment. Out of the less than 40% of companies that actually have an AUP, only about 10% are properly deployed. Experience, (usually bad), teaches users what works and what doesn't, and we have found in our investigations, that an improperly worded or deployed AUP is every bit as bad as no AUP at all.

A myriad of issues need to be addressed in any AUP, and we have tried to address the most important ones here. Obviously no two companies are alike, and any AUP will need to be adjusted accordingly.

The single most important consideration for any computer network must be security. Security above all else will dictate the freedom of access that any user will have over their computer. Most small businesses have nothing to govern the access their users have. A user can make changes to the computer, transfer data at will, and use the Internet to go anywhere they want, with no restriction. On the other end of the spectrum, high security installations, such as various branches of government, and R & D for large scale companies have extremely tight restrictions on what employees can do, and even go so far as to fill USB ports with epoxy so they cannot be used.

An AUP is not just for employees either. It needs to have direction in it regarding contractors that may use your network, either by sitting at your computers, or by connecting their own devices. Don't forget employees that use their own computers on the corporate network.

Security is a double edged sword that must be considered. At one end of the scale is convenience, and at the other end is security. The trick is to find the balance at which the two work for a company's applications. As well, it would be unreasonable to apply the same settings and rules to all computers in the network. Obviously the CEO, as well as a development department may need far greater access than a receptionist.

Deployment Considerations

Having an AUP is not enough. We have seen cases where a wrongful dismissal case was successfully won because the employee stated that although they had signed an AUP upon being hired 2 years prior, they couldn't possibly remember what it said. You cannot have an employee sign a piece of paper upon hiring, and expect them to remember its contents forever. You must have the AUP deployed in such a way as to ensure the employees always have access to it.

The most efficient way to do this is to have what is called a "click through" notice. In order for employees to log on to computers, they must first click their acknowledgement and agreement with the AUP. There should be a clickable link to the full AUP from this page. This completely eliminates the "I didn't know" argument.

How Much Internet Access and When

There is no question that employees would be perturbed if they were not allowed any access to the Internet. Having said that, if the employee has no need at all to use the Internet for their daily role, then why have it? It is possible in many different ways for an employee to send and receive email with no Internet access.

Arguments that have been brought up in court in the past have been things like how the AUP applies to coffee breaks, lunches, overtime, employees staying late on their own time, etc. While an unpaid lunch hour may very well be the employee's time, the computer and network used to access the Internet still belong to the company. If the employee inadvertently infects the network and causes a great deal of damage and downtime, the virus won't care if it was done on paid time or not. Purely from a security perspective, Internet activity needs to be strongly regulated no matter when the computer is in use.

Transferring of Data

Probably one of the most prevalent abuses seen in the corporate world is the theft of proprietary data. Very common also, is the destruction of corporate data by a disgruntled employee. An AUP should outline what access, if any, an employee has to the data storage areas of the network, as well as what the rules are pertaining to removing it from the network. AUPs should address the deletion/destruction of files as well.

Connecting Devices

Any AUP needs to address the connection of external devices to the computer. Are employees allowed to use their USB thumb drives on any computer in the network? How about outside CDs or DVDs? A very common example of corporate espionage today involves loading a number of USB drives with malicious programming that will open a back door into the network. These USB drives are then randomly dropped somewhere where employees will find them, such as the coffee shop in the building lobby, or around the elevator on the company floor. This technique is more commonly known as "salting". Human nature is such that the first thing we want to do is plug it into our computer to see what is on it. Once plugged in, it is too late, and the malicious programming automatically deploys. It is also possible to allow USB devices, but set the computers up so that data transfer is one way. In other words, users can move data FROM the device TO the computer, but not the other way.

Changing Settings

Your AUP should give direction on what a user is allowed to change or modify on their computer. Most AUPs have a blanket policy that bars users from changing any settings. This is a good policy, but again this is one area that a lot of damage can be done. By accidentally changing a setting (or intentionally), a user can cause thousands of dollars of damage to a network. Viruses can be injected into a system through something as innocent as changing a screensaver or the desktop wallpaper. As well, a common monitoring program found in Windows networked computers can easily be shut off by a couple of mouse clicks.

AUP Augmentation

Although an AUP should be an integral part of any network environment, it is not a panacea. It should be backed up with proper network administration. Most every issue I have addressed in this article can be further enforced by proper permissions deployment across the computers in the network. A very brief list of settings that can be controlled include:

- When the Internet can be accessed, if at all
- What websites can be accessed and which ones cannot
- What settings a user can change on their computer
- What programs can be accessed and when

- What devices can be connected to the computer, if any

Although some of the above may sound draconian, the employer must first ask themselves what they have to lose if the above is not followed. Without a properly advised and administered AUP the employer might also find themselves on the wrong end of Federal Wiretap Laws. Acceptable Use Policies have not developed simply because somebody had extra time on their hands. Sadly they have been born of necessity.

Important: The above information is the sole opinion of the author and NOT legal advice in any capacity. Seek legal advice from your attorney before acting upon any of the information contained in this article.

Kevin J. Ripa is the President of Computer Evidence Recovery, Inc, and has been involved in numerous complex cyber-forensics investigations. He can be contacted via his website at www.computerpi.com.

Florida PI Conference

The Florida Association of Private Investigators, Inc. will be holding its annual conference and litigation seminar in Orlando, Florida at the Wyndham, Lake Buena Vista, October 13th - 16th. Guest speakers will include Judge Marc Lubet (Female Astronaut Case), attorney Mark Rabinowitz (Expert in Domestic matters and the use of an investigator to assist in domestic cases), Brian Ingram and Kevin Ripa on forensic computer investigations including email tracing, and other interesting speakers yet to be announced. There will also be an exhibitors' room with the latest in electronics, books, database searches, insurance products and so forth. Room rates are an astounding low of $59 plus tax including free Internet, microwave and refrigerator. This is an official Disney Hotel with free shuttles to Disney properties and Disney characters for the children. Conveniently located near all Central Florida attractions and the Orlando International Airport. Registration information is available at: www.myfapi.org

Pinging a Cell Phone: Fact or Fiction?

John B. Minor
Atwater Enterprises
Odessa, Texas

Throughout the cyber-world myths abound regarding the ability to "ping" a cell phone and determine its real-time geographic location. Virtually all cell phone carriers worldwide have implemented Location Based Services (LBS).

Within the United States, and outside of the U.S. intelligence community and the FBI's Carnivore or DCS-1000 – Red Hook or DCS-3000 – Digital Storm or DCS-6000 – secret DCS-5000 DCSNet lawful intercept tool capabilities & usage, in only four scenarios can lawful real-time cell phone tracking of geographical location occur.

Sadly, some companies claim to be able to perform real-time "ping" geo-location tracking of almost any cell phone. Uninformed buyers are often told that the cell phone is "being pinged" but has not answered and expenditures for these scams, ranging up to hundreds of dollars, are often unsuccessful and seldom refunded.

Lawful Cell Phone Real-Time Tracking Scenarios

Scenario 1: During an E911 call from a cell phone the geo-location of the device is determined and transmitted to the 911 call center. Documentation or evidence of the geo-location event is available under the Freedom of Information Act. The reported location varies from a few feet to several square miles depending on which cell phone carrier is involved, the number of cell sites in the general vicinity of the cell phone and, finally, the geo-location calculation technique successfully employed during the location calculation.

Scenario 2: Federal Law Enforcement can perform real-time geo-location tracking, under minimal judicial supervision, using carrier portals available only to Federal Law Enforcement. For example, Sprint's Law Enforcement Portal performed over 8 million real-time locates in 2008. Today, use of this technique is even more common.

Scenario 3: A cell phone can be located real-time using a procedure called an "idle mode query" (IMQ). Declaration of exigent circumstance to the carrier can escalate the IMQ to immediate for LE or others with the technical knowledge and authority to act. An example would be an emergency locate for a missing person's or deceased victim's cell phone.

Scenario 4: Location based services are in use by all carriers and, depending on the cell phone model and applications in use on the cell phone handset, real-time geo-locates can occur during regular usage and can thus be utilized to perform a real-time locate on the cell phone by anyone gaining access in this manner including friends, investigators and criminal stalkers. Example applications are the family plan locate services offered by carriers, social networking applications that, if enabled, allow a real-time locate to occur when in use. Real-time and historical trend geo-location tracking is a very real possibility when social network applications such as MotionX, Facebook Places, Foursquare.com, Gowalla.com and Scvngr.com are in use by a cell phone subscriber. Geo-Tagging photos from a mobile and then uploading the images to Flickr or Picasa can also result in historical trend geo-location tracking. A relatively unsophisticated perpetrator can figure out where a target lives, works, socializes and much more using simple trending analysis techniques. Loopt provides cell phone based GPS social network sharing that enables subscribers to visualize each other's location and share information. Many other similar examples exist.

Unlawful Cell Phone Real-Time Tracking Scenarios

Scenario 1: Unlawful tracking of cell phone geo-location can occur if spyware has been installed in a cell phone. Spyware installations are difficult to detect. Monitoring by an expert of cell phone handset communications can confirm the presence of spyware.

Scenario 2: Although several vendors claim to be able to remotely access a cell phone via the Bluetooth communications port, this technique more often ends in failure. Bluetooth has a range of only 10 meters however "rifle" technologies enable targeting Bluetooth devices at much greater ranges.

Outside the United States

Location Base Services have been implemented by most cellular carriers around the world. Access to geo-location information is determined by local laws, directives or mandates.
Cellular carrier Location Based Services can be exploited globally to perform geolocation services for a subscriber cell phone by a disciplined investigator accessing commonly

available location information disseminated by less discrete cell phone subscribers using resources from Scenario 4 above.

The services of a communications expert are highly recommended when venturing into the world of real-time or historical communications device geo-location tracking.

About the Author – John B. Minor is a practicing communications & lawful intercept expert, cell phone signals analyst, digital Investigator and forensic examiner. John has leveraged major successes for litigation & investigative teams by locating digital evidence under unusual scenarios.

Four Month Intellenet International Investigation

David Ziegler
Ziegler and Associates
Titusville, New Jersey

Intellenet together with New Jersey based member David L. Ziegler, CFE, CFI, VSM initiated a joint venture with a large international firm as part of our Director's initiatives to assist our members in file development. This NJ based firm conducts audits throughout the world for a major client.

Ziegler and Associates, Inc. is contracted by the firm to identify, retain and coordinate with Intellenet members to conduct audits and investigations in the United States and around the world. Intellenet member Adrian Charles through his firm, JLA Security, recently completed a long and difficult assignment in China (PRC).

This four month assignment conducted in Shanghai required his field investigator to identify, confront and interview a suspect who had stolen a sensitive proprietary information from the client. The investigator had to change course and techniques several times during the investigation to keep up with the suspect and his activities. This type of theft calls into question the entire product integrity of the client's product and could be used to make large profits for the subjects behind the theft.

Adrian's firm and field investigators were able to confront the suspect, obtain a confession and retrieve the proprietary materials. This is just one example of the international reach and great work of our association.

Recent US investigations have also been completed in Dallas and Keller, TX and Walnut, CA.

Video Surveillance Evidence: Are Digital Copies Admissible?

F. Scott Harrell
Compasspoint Investigations
Gulf Breeze, Florida

(Originally published by the author in *Pursuit Magazine*. Reprinted by permission of the author)

Recently, a private investigator posted the following in an association's listserv to which I belong and it raised some seriously interesting responses:

"Technology is advancing rapidly in the digital video camera market and our clients expect crisp high definition video as opposed to the fuzzy standard definition video we are capturing on video cassettes right now. All of the new cameras coming into the market are using SD memory cards and internal hard drives.

My question is this, if I capture surveillance footage to an SD card and then download it later to a computer and that footage is then burned to a disc, is there any reason why the footage from the disc would be disallowed in court? Does the original SD card need to be preserved?"

The first five or six responders were very adamant about keeping the original SD (Secure Digital) cards and anything less they asserted was the spoliation of evidence. There were several comments about maintaining video evidence logs and a chain of custody receipt too. One investigator had the audacity to go against the popular consensus and took the position that a disc-copy made in the manner described would be perfectly admissible.

Here is a response from one listserv member that pretty much summed up what everyone else was saying:

"The golden rule of evidence is that you ALWAYS keep the original, no matter what, period! Additionally, of equal importance is the Chain of Custody. If you collect evidence that may end up in court, you must have established procedures regarding the collection and preservation of that evidence; when was it seized and by whom?"

Well, my opinion is that it's not really all that simple or complicated (depending upon your point of view) and I thought it was time to throw my own reply into the conversation.

First thing's first: The question is for those of us "in the now," not where we've been.

What I mean is this – professional private sector investigation is ENTIRELY different than law enforcement-related investigation, where the goal is to win a criminal conviction and put the bad guy in jail. When it comes to a question about evidence some ex-law enforcement guys are really quick to cite their relevant, past, experience and then, almost without fail, they use the terms "Best Evidence Rule" and "Chain of Custody," which they are taught in their respective academies. Rightly so, putting criminals in jail requires an extraordinary level of care and attention to detail when working with evidence headed for the criminal justice system. However, if you are a private investigator now, then you are working on behalf of a client on a civil matter (criminal defense investigators excluded) and the standard of care is altogether different.

I believe that to better answer the original question we have to first establish the circumstances in which the surveillance documentation is obtained and identify the purpose it will ultimately serve.

I start with the assertion that most of us here are private investigators now. For the general purposes of this discussion very few of us are in the business of obtaining evidence that will be directly used to build a criminal case against a "suspect" that will then be turned over to

a prosecuting attorney who will use that evidence in a criminal trial replete with all of its nuances, like chain of custody issues, testing and validation or "fruit of the poisonous tree."

No, instead we are using surveillance video to document a person, place or thing so that our client can evaluate that documentation in the context of whatever questions he or she has- be that watching his or her spouse with another love interest, evaluating a claimant's actual daily activities and physical appearance against a stated claim, documenting an employee's behavior while on the job, etc. etc.

So I am going to limit my comments to those few areas where video-based evidence is used most often in civil law courts where we attempt to right a wrong, honor an agreement, or settle a dispute:

- claims-related and AOE/COE assignments,
- documenting the location where an accident or crime may have occurred,
- questions of infidelity,
- child care & custody issues,
- potential incidents of employee theft and
- some intellectual property disputes.

While I can agree with many of my colleagues that "Best Evidence" would be the original SD card, I would also submit that we have to consider video and it's practical application in real-world scenarios rather than what "the book," and all those who subscribe to it out of necessity, might have to say.

"Best Evidence" rarely comes up, if ever, when applied to the source of video documentation in common private investigation assignments. Even if it did, one would only need to look as far as the Federal Rules of Evidence, Article X, Rule 1001 for clarification on the terms, "*Original*" and "*Duplicate*" as it might apply to the "Best Evidence Rule" in reference to digital video evidence:

ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS:
Rule 1001. Definitions

For purposes of this article the following definitions are applicable:

1. Writings and recordings. "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
2. Photographs. "Photographs" include still photographs, X-ray films, video tapes, and motion pictures.
3. Original. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".
4. Duplicate. A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by

> chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

In preparing this article I scoured Lexis-Nexis countless hours looking for a citation from case law where digital video documentation was disallowed in a civil trial because the source media was not produced; I could find nothing at all. In the absence of having case law or precedent from which to learn, I like to throw out the theory and rely instead upon empirical evidence:

I have only been at the surveillance game now for about 15 years, not as long as some of you I know, but claims-related surveillance is the mainstay of my agency. We do not handle digital forensics, criminal defense, personal injury cases, etc. In 2009, I upgraded all of our video cameras to high definition digital video cameras with on-camera memory and an SD slot for extra storage, meaning that we no longer use tapes and have not since February of 2009.

Since converting to all digital video cameras, our usual work-flow after the surveillance day is over is to download all (100% – warts and all) of the video documentation obtained from the camera to a computer. That file is then burned to two DVDs. The video is unedited and all of the metadata is preserved for later scrutiny if warranted. Those DVDs are clearly marked as "unedited;" one copy always goes to the client and we keep the other.

The video documentation on the computer is then edited to the client's specifications; we throw in some titles and essentially create a "highlight reel" so that the client can quickly evaluate what he or she has and how it affects his or her case, claim, job, life, and marital status… whatever. Most of our claims-related and county/municipal clients now request that we upload the unedited video so that they can watch it online and distribute it accordingly. The unedited-uploaded video is usually what the opposing party gets in discovery.

With all of that having been said, here's the substance of where I am going:

Since making the transition to digital video cameras my investigators and I have completed several hundred days of claims-related surveillance assignments, have been to deposition a few dozen times and testified in trial on numerous occasions. Because many of our cases are related to offshore injuries (Jones Act) we testify regularly in Federal courts. Of course, we do a couple dozen infidelity or child custody cases and the odd employee theft assignment here and there every year as well.

In that same time period do you know how many times we have been asked why we did not, or could not, produce the original source's SD card, videotape or other first-generation media storage (like the camera's on-board flash chipset)?

Zero, not once.

When we converted to digital I probably built up an inventory of SD cards worth over $750 so that we could keep the original video file. It eventually became apparent to me that no one cared about the source media, so I started asking questions why. Universally, the attorneys and claims adjusters could really care less as long as we gave them the raw and unedited video, or at least kept it somewhere safe until the claim had been settled or litigated. The name of the game is efficiency and expediency- from the adjusters, to the

attorneys to the court room. From the time a matter is brought up until it is settled or litigated there is really only one question on their minds:

What does the video depict and what does it mean?

But Scott, your copy of the video evidence may not be forensically sound and would lose all probative value!!!

"Forensically sound" is a wonderful concept when you are trying to get digital evidence disallowed in a criminal defense investigation because it casts doubt upon the competency of the person collecting the evidence and/or the methods used to collect and preserve the evidence. The reality of video in a civil trial, however, is vastly different. You cannot cast doubt on the competency or methods of the guy who turned his video camera on, pointed at something, recorded some video and then made that video available for your viewing pleasure. It's been tried and beaten many, many times when (analog) video surveillance footage found its way into the courtroom.

The probative value (*"Is something sufficiently useful enough to prove or disprove something important?"*) of video documentation really boils down to the threshold of "it is what it is."

Video-based evidence, for the run-of-the-mill private investigator and our client's needs, stands on its own merits in all but the rarest of occasions if it meets a few criteria:

- Was the video documentation obtained lawfully?
- Can the trier of fact view the video and positively identify the subject?
- Is the video's quality clear and stable enough so that the trier of fact can evaluate the subject's activities or condition in context of the matter at hand?
- If these criteria are met, what does that video prove or disprove (if anything)?

In claims-related assignments the claimants/plaintiffs always want the unedited copy. We are almost always asked under oath if the unedited video documentation is complete and represents everything we obtained during the course of our investigation. We say yes, and that's that. They move on.

No one is out there manipulating video in order to make it magically appear that a disabled claimant is clearly not walking with his "much needed" cane or working a roofing job though he adamantly denies being able to work. When was the last time you heard of a PI using CG wizardry to make it appear that some guy's wife is doing the horizontal boogie with the pool boy so he or she can say they hit a home run for the client?

Zero times.

It doesn't happen. You all know it and the attorneys all know it. The idea of contrived video footage is old and thread-worn.

What DOES happen occasionally is that some investigators may not provide the complete and unedited version of the video obtained while on assignment because they caught some seemingly inconsequential footage that was obtained by an inadvertent press of a button, is out of focus, terribly shaky or the horizon was 45 degrees from level for a few moments. Ethically and professionally that is wrong by any standard. It becomes an entirely different

matter when the investigator swears under oath that the documentation provided was obtained by him or her and represents all of the video documentation obtained during the course and scope of his or her investigation.

I'll make this last point:

In the 15 years and hundreds of depositions and trials in which I have provided testimony, I have also never been asked for a chain of custody log for my videotapes or discs.

Again, that's ZERO times.

(*Sure, I kept one for several years back in the mid-90's but I was a bit wet behind the ears back then.*)

We do however, keep an inventory sheet of all of the videos we do have so that we can periodically verify that we haven't lost anything… That's just good business.