INTELLENET QUARTERLY

December 2011

TABLE OF CONTENTS

Carino's Corner

James P. Carino, CPP, VSM
Executive Director

As 2011, our 28th year, draws to a close, we note it was another very successful year for Intellenet. New member recruitment efforts with only minimal non-renewal losses further improved and expanded our worldwide coverage and responsiveness not only for members to render investigative support but also in providing investigative assistance to a growing number of corporations and businesses throughout the world. Several new member initiatives regarding business development were the primary driving forces behind membership expansion and investigative opportunities.

The year 2011 was Intellenet's entry into the publication field as many members prepared Chapters in two books – one addressing basic skills and one advanced skills for private investigators. Both books have been well received in the marketplace. A third volume is scheduled for publication in late spring 2012. All are available through the publisher, Charles C. Thomas.

Also, Intellenet's Speaker Bureau, initially established in 2009 was further updated and expanded. Many Associations have called upon our members to serve as conference presenters to great benefit and advantage. Our Speaker Bureau list is now on our www.intellenetwork.org website under its own menu item caption.

Plans are progressing nicely for our 2012 Conference on 16-19 May 2012. A great Canadian Rocky Mountain train ride to Whistler with great local professional presentations and an old fashioned BBQ are two of the many highlights scheduled. Registration info would be out shortly but mark your calendars for a terrific networking, educational and social extravaganza.

Goals for 2012 include further increasing our membership through selective worldwide recruitment (with special emphasis on international resources), fruition of several initiatives regarding worldwide investigative opportunities/assistance and increased exhibiting at relevant conferences.

Season's Greetings and best wishes to all for good health and happiness in the coming year.

Members in the News

Werner Preining, Vienna, Austria, is this year's award winner for the prestigious Bordes Award issued annually by ASIS International for outstanding achievement in the furtherance of ASIS. **Sandra Stibbards** will be on the road doing a series of presentation on Open Source Intelligence and 1-2 day seminars in San Francisco (The Computer Forensics Show, October 18-19) Washington, DC, November 2-3, Torrence, CA, November 12, and Las Vegas, December 6-7. **Jim Hilton**, Hilton Investigative Services, Raleigh, NC, is on the ASIS International Investigations Council. **George Michael Newman,** recently had two article published in *PI Magazine.* **Werner Preining**, Vienna, Austria, was a speaker at the ASIS Malaysia Conference. **Tom Miles**, Germantown, TN, recently authored an article for *PI Magazine*. **Nicole Bocra**, Arlington, VA, and **Kevin Ripa**, Calgary, Alberta, were speakers at the Paraben Forensic Innovations Conference in Park City, UT.

Know Your Fellow Member

David G. Duchesneau, CII, CFC
Standa, Inc.
Milton, New Hampshire

David Duchesneau has over 40 years of experience as a government law enforcement officer, detective, New Hampshire State Trooper, and private investigator. He is a graduate of the FBI National Academy and specializes in database research, surveillance, corporate internal investigations and vulnerability assessments.

New Members

Sergey Grudinov, Moscow, Russia; Malcolm Brammer, Integrity Risk Solutions, Castle Hill, NSW, Australia; **Mark Gillespie**, Gillespie Investigations, LLC, Cedar Park, TX; **Gerardo Cappuccio**, Vives Investigations & Risk Management, Avellino, Italy

Staffing and Maintaining a Compliant Special Investigation Unit (SIU)

Jack Scott
SIU Investigative Services
Spring Hill, Florida

As of 2011, nine (9) states actually require insurance carriers writing specific lines or certain volumes of business to have an in house SIU or contract SIU. Many of these states use the terminology, "adequate SIU". Twenty-two (21) states require insurance carriers to have a fraud plan and have specific areas of responsibility which need are designated to assigned to an SIU unit. Yet, annual reports of insurance regulator's anti-fraud audits and market conduct reports consistently cite findings that carriers SIU are "inadequate or non-existent", "SIU investigation procedures are inadequate" and "lack of continuing training for the SIU staff."

Carriers should review the statutes and regulations for each state they are admitted to ascertain their SIU meets the proper criteria. Several States have set minimum standards and training requirements for the SIU staff. It is recommended that Carriers, who do business in multiple states, utilize the most stringent States requirements in developing internal responsibilities for their SIU unit. After reviewing the current requirements of all the states which mandate SIU units, carriers should consider the following issues.

- The SIU unit must operate independently of the claims and underwriting departments.
  The reasoning is that the claims process should not be impeded or altered due to an SIU Investigation. The SIU unit's responsibility is to determine if the activity presented constitutes fraud and take the appropriate action to deter or expose the fraud. The mere fact that the claim is assigned to the SIU does not warrant denial of the claim. As an independent unit, the SIU should work with the claims unit but not be directed or supervised by the claims staff.
- An SIU Investigator must have at least 5 years investigative experience
  In order to insure that SIU investigators have ample experience the above guideline was set up. Certain educational and other select experience can reduce the number of years experience in most states. This requirement does not extend to a surveillance investigator or field investigator. The requirement pertains to SIU Investigators who review, handle and investigate suspicious claims. Some carriers utilize their investigative vendor as a contract SIU to handle suspicious claims. In these cases the carrier must be certain that the investigator assigned meets States standards.
- An SIU Investigator must have at least 9 hours of advanced Anti-Fraud training each year.
  Many SIU Investigators are also Anti-Fraud trainers. This also means they have to keep up with new insurance fraud trends, fraud fighting tools and program to enhance their value as a trainer. During the course of a recent audit, the state agents would not recognize the carriers in-house attorney, Compliance officer or Executive officer as an SIU team, member. They cited the fact that these staff members did not have adequate investigative experience but more importantly they did not have adequate advanced annual anti-fraud training.

- The SIU Investigator should be the "gatekeeper" for any information shared with law enforcement, State Insurance fraud units and other carriers.
  State statutes provide specific conditions where information can be shared. In these instances, it is important that the carrier be protected from litigation by use of "immunity" Statutes. The SIU investigator is trained in the proper applications of these statutes.

Regulations and experience dictate many issues which need be considered in building and staffing a compliant and effective SIU Unit.

- The SIU Unit is responsible for creating programs to detect, prevent, and investigate fraud. They are also assigned responsibility for Anti-Fraud training and awareness. Staff members need to be assigned with skills beyond just surveillance and investigation.
- Investigators with both civil and criminal experience are best suited for SIU Investigations.
- The SIU management function is always more effective at the carrier level, especially for compliance issues. This is especially important where numerous TPA's are involved for a carrier. Carriers are permitted to contract their Anti-Fraud programs to a TPA; however, the responsibility for non-compliance, violations and fines rests solely with the carrier.
- In most every state, the costs of Anti-Fraud compliance and the overhead costs for an SIU unit is chargeable to the carrier's administrative line for rate increases. The cost of individual claims investigations is only chargeable to the claim.
- Once a file is determined to be suspicious, the SIU should take the lead in furthering the investigation. They must stay in contact with the appropriate referring personnel
- The SIU staff is responsible for investigating suspicious activity. In most instances it is more cost effective to use outside vendors for claims investigation such as witness statements, document retrieval and surveillance. If a claims investigation reveals suspicious conduct, it can then be assigned to the SIU unit.
- The SIU should be an intricate part in rating, approving and monitoring (quality control) of outside investigative vendors. This is sometimes referred to as vendor management.
- It is preferable to have more than one outside investigative vendors to maintain competitive pricing, service and quality standards. It is not always a good practice to allow sole source vending.
- It is preferable to utilize an outside investigative vendor for internal investigations involving staff personnel when litigation could be involved. This procedure displays and "arms length" independent investigation. It precludes the defense from casting doubt on the integrity of an investigation by the company's in-house staff. It also alleviates any breakdown of "trust" between the SIU unit and other staff members.

The above described information should be considered in the staffing of the in-house or contract SIU unit. Annual updates of the SIU staff qualifications and training is recommended. Although carrier's particular state(s) of admission dictates actual compliance, the stated guidelines should be considered as "best practices". These "best practices" will become the structural models for other jurisdictions as they expand their Anti-Fraud Statutes and regulations in the future.

Jack Scott, a member of Intellenet, is an Anti-Fraud Consultant with SIU Compliance Solutions Inc. He completed a 20 year career as a Detective with the Suffolk County Police NY. He has in excess of 17 years of experience assisting carriers in developing cost-effective compliant SIU/Anti-Fraud programs. Several of his clients have been carriers licensed in all lines and all states. Jack is recognized by many in the Insurance Industry as an expert in Anti-Fraud compliance issues.

Special Investigation Unit Guide

Jack Scott
SIU Investigative Services
Spring Hill, Florida

Special Investigations Units (SIU) are required in the following states:

Arkansas

- Insurers shall have antifraud initiatives reasonably calculated to detect, prosecute and prevent fraudulent insurance acts. Antifraud initiatives include, but not limited to: Providing fraud investigators, who may insurer employees or independent contractors;

  Sec. 7. Fraud Investigators and independent contractors

- Shall be qualified by education, experience or training in the detection, investigation and proper reporting of suspected fraudulent insurance acts, and may be employees whose principal responsibilities are the processing and disposition of claims, if they meet the qualification requirements herein stated; and shall complete a minimum of three (3) hours of continuing education annually in the detection, investigation and proper reporting of suspected fraudulent insurance acts. The specific curriculum, location and certification of said continuing education courses are not mandated but shall be consistent with industry standards for continuing education for insurance fraud investigators.

California

State Insurance Code Section 1875.20 (Fraud unit required); Administrative Code - Title 10 Section 2698.42 (Purpose and objectives of insurer special investigative unit).

- Every insurer admitted to do business in this state shall maintain a unit or division to investigate possible fraudulent claims by insureds or by persons making claims for services or repairs against policies held by insureds.

- "Special Investigative Unit" (SIU) means an insurer's unit or division that is established to investigate suspected insurance fraud. The SIU may be comprised of insurer employees or by contracting with other entities for the purpose of complying with applicable sections of the Insurance Frauds Prevention Act (IFPA) for the direct responsibility of performing the functions and activities as set forth in these regulations.

  Section 2698.32 SIU Staffing

- Adequacy. The adequacy of an insurer's SIU staffing shall be determined by its demonstrated ability to establish, operate and maintain an SIU that is in compliance with these regulations. Factors that may be considered in staffing the SIU include, but not limited to, the number of policies written and individuals insured in California, number of claims received with respect to California insureds on an annual basis, volume of suspected fraudulent California claims currently being detected and other factors relating to the vulnerability of the insurer to insurance fraud.

- Knowledge. An SIU shall be composed of employees who have knowledge and/or experience in general claims practices, the analysis of claims for patterns of fraud, and current trends in insurance fraud, education and training in specific red flags, red flag events, and other criteria indicating possible fraud. They shall have the ability to conduct effective investigations of

suspected insurance fraud and be familiar with insurance and related law and the use of available insurer related database resources.

Colorado

- Each anti-fraud plan shall outline specific procedures, appropriate to the type of insurance provided by the insurance company in Colorado, including: provide for the hiring of or contracting for one or more fraud investigators.

Washington DC

- Employment of fraud investigators: D.C. Code 22-3825.9 (a)(3). The anti-fraud plan should contain specific procedures for determining who should conduct or oversee such investigations.
- You should analyze your options to maintain an in-house staff of investigators or contract with an outside firm.

Florida

- Requires carriers writing more than $10 million in direct written premium in Florida, to have a Special Investigations Unit (SIU).
- The SIU is to be responsible for the investigations of suspicious insurance fraud issues.
- Those writing less than $10 million in Florida premium can maintain an SIU, or they may file and anti-fraud plan instead maintaining an SIU.
- Carriers may utilize a qualified contracted SIU or maintain an in-house SIU.

Kentucky

KRS 304.47-080 —

- Every insurer admitted to do business in the Commonwealth shall maintain a unit to investigate possible fraudulent claims by insureds or by persons making claims for services or repairs against policies held by insureds.
- Insurers may maintain the unit required by subsection (1) of this section, using its employees or by contracting with others for that purpose.
    - The unit may include the assignment of fraud investigation to employees whose principal responsibilities are the investigation and disposition of claims.
    - If an insurer creates a distinct unit, hires additional employees, or contracts with another entity to fulfill the requirements of this article, the additional cost incurred shall be included as an administrative expense.

Maine

- The antifraud plan must outline specific procedures include providing for the hiring of or contracting for fraud investigators

Maryland

- Insurance code does not require carriers to staff an in-house SIU.

- Carriers Anti-Fraud Plan must identify the individual or specific department, either in-house or qualified vendor, who will be responsible to administer the Anti-Fraud Plan and investigate suspicious insurance fraud issues.

- A Fraud Manual must be available for each adjustor, underwriter and agent. The manual must delineate for its staff the carriers policy and procedures in their Anti-Fraud Plan.

New Hampshire

- Every insurance company licensed to write direct business in this state shall have antifraud initiatives reasonably calculated to detect, prosecute, and prevent fraudulent insurance acts, including: Fraud investigators, who may be insurer employees or independent contractors.

New Jersey

- Carriers who write less than 1000 NJ auto policies or less than 10,000 NJ health or life policies are exempt from being required to have an SIU.

- All other carriers who meet the above threshold must have an SIU.

- NJ additionally describes special provisions for the quantity of SIU staffing, qualifications of SIU staff and advanced training requirements for the SIU.

- Qualified contract SIU vendors are permitted.

New Mexico

- Every insurer who in the previous calendar year reported ten million dollars ($10,000,000) or more in direct written premiums in New Mexico shall establish, prepare, implement and submit to the superintendent an anti-fraud plan that includes provide for the hiring or contracting of fraud investigators.

New York

- Requires all licensed carriers, collecting premium in New York State, to maintain and in-house or a qualified SIU vendor.

- NY special requirements for SIU's which includes: experience qualifications, minimum training requirements and mandates the SIU must not report to or be part of the adjusting or underwriting departments.

- A senior executive of the carriers must be accountable for the SIU.

Tennessee

Every insurer with direct written premiums exceeding ten million dollars ($10,000,000) shall prepare, implement, and maintain an insurance anti-fraud plan. Each insurer's anti-fraud plan shall outline specific procedures including providing for the hiring of or contracting for fraud investigators.

---

*Note- twenty-two states require carriers to have an Anti-Fraud plan, described by either statute or regulation. In most every instance, an SIU is mentioned or designated to be assigned certain responsibilities within the Anti-Fraud Plan. It would appear that it would be a "best practice" for carriers licensed in those states to have a compliant SIU also. This guide was prepared by reviewing individual states insurance statutes & regulations in addition to a decade of anti-fraud compliance experience. It is offered as a guide for informational purposes only. Any formal legal opinion should be obtained from legal counsel or directly from the appropriate state regulatory unit.

Thank You for Your Assistance

Bill Blake
Blake and Associates, Inc.
Littleton, Colorado

Starting with Intellenet Quarterly March 2012 issue, Don Johnson, Trace Investigations, Bloomington, Indiana, will become the newsletter editor. We started the electronic issue of the Intellenet Newsletter in September 2005 and all issues can be found on the Intellenet website, www.intellenetwork.org. I want to thank everyone who contributed to making the newsletter a success.

Simple Suggestions for PI Safety and Security

Tom Miles
The Hawk Company
Germantown, Tennessee

As private investigators, we have a perpetual obligation to serve our clients and case affairs with an unwavering dedication, cost-effective procedures and optimum efficiency. However, in doing so, we sometimes tend to slight ourselves by disregarding our own personal safety and security. All investigators, whether self-employed or with corporations, have established procedures for client contact (initial or subsequent), record controls, interview techniques, report formats, etc. But one special factor – a private investigator's basic welfare – is frequently ignored during the concerted efforts, singular or corporate, in resolving case issues and appeasing clients. Perhaps the following suggestions might be worthy of adoption or helpful in generating even more ideas.

1. Back up everything on your computer, and do it immediately for case activities! A PC crash can occur at any time for many different reasons. Personally, I use *Carbonite* as an excellent and reasonably priced system. But I also back up my case files on an external hard drive, flash drives and CD's or DVD's. Furthermore, since the life span of CD's and DVD's is not precisely known and they are susceptible to damage, I routinely refresh their contents by making new ones about every other month or so. Additionally, I enter all case files into a second PC…one which is held in reserve but not online…so that I can quickly get back online in the event of a crash on PC #1.

Whether you're self-employed or a corporate team member, every PI must always be sensitive to the absolute necessity for maintaining accurate and encompassing case notes, records and files. Furthermore, investigators should embellish records and files by any legal means available. If your state laws allow the tape recording of phone conversations, do so as deemed necessary –and "flag" the dates and times by inserted references to things like newspaper headlines of the days *before and after* the action, TV or radio station broadcasts etc. Tapes can be spliced, and phone chats can be challenged in or out of court. So be certain that you can prove timing and continuity. Any reckless recording of calls can place you or your firm in serious jeopardy.

2. Memos. For each and every case, my standard practice is to write two memos for each case folder. The first one is a Memo for File (MFF), a simple log with abbreviated phonetic spelling on all case information – client name; date of contact; case circumstances; date of engagement; contact addresses and phone numbers; client requests; case proposals; phone calls; emails; etc. The MFF is encoded and never shown

to anyone – it's a private guide to bolster productivity and a reference item for constant reviews of case meetings, actions taken, procedures and results.

The second memo is a Memo for Record (MFR). This particular type of memo, based on client needs or developing case conditions, is designed for publication or release without the hindrance of formal correspondence. For example, an MFR can be used as a cover sheet for any documents reflecting immediate attention. MFR's are dispatched to a client by courier. This is well worth the trivial cost; it saves time in preparation and submission. You never know who might see a Fax transmission or an email attachment. Couriers are more secure, they're fast and the given recipient can easily study a concisely worded MFR with its attached papers while you, in turn, gain irrefutable proof of the delivery by date and time.

3. Get a small tape recorder, and never leave home without it. In performing case work, a tape recorder is an exceptionally helpful item. Use it for thoughts and ideas; for notes and reminders of things to do; for the accurate logging of mileage and time on future invoices; for a general reference (etc. weather conditions, case activities, unusual events, etc.) Upon leaving home, I'll log what I'm wearing; cash on hand, the case file name, the date and time and even the headline for that day's newspaper. The next day I'll log that day's headline. Again, tapes can be spliced. However, that last action stands as an indisputable proof of the day, date and time frame when something occurred or was accomplished. I also log mileage and time for all stops made plus the next destination upon my departure from any given location. Ultimately, such recordings provide optimum accuracy and efficiency in writing reports and in compiling invoices. A tape recorder might also be a crucial aid in coping with emergencies. Here's how:

4. Anticipated or not, investigators sometimes tread into danger -- neighborhoods known for their high crime rates or encounters with hostile people. Lone travel by car might also involve risks such as an accident or a sudden illness. As a routine gesture for both safety and security, I always leave an envelope at home before striking out on case duties and a note inside explains the gist of my venture – where I'm headed, with whom I'll be meeting, etc. If I'm incapacitated for any reason or fail to return on time, my family can quickly take appropriate action.

Aside from notes left behind and the highly recommended usage of a tape recorder, there is another consideration for the travels of lone investigators – to be armed or not to be armed.
The carry of firearms by a PI is a very debatable issue. Essentially, though, it's a matter of personal choice, blended in full compliance with regional area laws, individual responsibility
and an awareness of the pros and cons applicable to all circumstances at hand. As a general rule, especially for high crime neighborhoods or lengthy road trips through cooperative states having agreements of reciprocity for hand gun permits, I'm usually armed. (Yes, even the weapon serial number is memorized and declared by make and model on my tape recorder as I leave home.)

In the past twenty years, I've been mugged no less than four times and I've also intervened and halted two armed robberies in progress. The police were promptly notified, of course, after each event. But I never fired a shot. On each occasion, fortunately, it was quite sufficient to either brandish my holstered firearm or draw it. Regardless of supportive or opposing feelings about going armed, the points to be noted are the regional laws for case activities and an investigator's decision with respect to proficiency and total appreciation of potential consequences for usage.

Strengthen Your Business, Develop Your Investigative Niche

Sandra Stibbards
Camelot Investigations
Aurora, Colorado

The investigation industry offers a wide range of opportunity for work. The case options as a licensed investigator vary from surveillance, interviews, accident reconstruction to due diligence, backgrounds, asset investigations to intellectual property, counterintelligence, or corporate espionage investigations. These are just a few fields to consider. But, as a licensed investigator, you can't do it all on your own.

Advertising and marketing your investigation agency is an important step to expand your business. A powerful way to market yourself is to specialize in an investigative field that makes you stand out and be remembered by your clients. Attorneys and corporations will hire an investigator to handle a specific case situation. They will continue to hire the agency that is capable of taking care of their needs and getting the investigation done correctly. Determine your strengths and build on them. Specializing in a few aspects of investigation will make you lead the way in your field and provide the client insight that your agency is the one to hire when in need for that specialty.

Although other investigative agencies may be considered competitors, keep in mind they may also be colleagues who specialize in other fields of investigation. Utilize those colleagues and develop a trusted network. This will provide your agency the option to take on all types of investigations. Determine which agencies specialize best in each type of investigation. Develop a solid business relationship with those that you work with well. These various contacts within your network provide you the ability to offer a wide range of investigative services to your clients.

Fraud investigations, being one niche, can span into several fields of investigative needs. For example, a multi-million dollar embezzlement case will most likely require more than a specialist in financial fraud. Once the target has been identified, located, and the embezzled funds found, additional work is required. Quite often this type of case becomes international. The financial fraud investigator would need assistance with seizing funds in the international location and surveillance may also be required. The trusted network the fraud investigator has developed in these fields of investigation will be able to assist. The client will know the agency is capable of handling all areas of these investigations as well as realize the international capabilities.

Options to learn and develop a specialized field of investigation are available. Searching the internet for free webinars and paid webinars can make it simple and affordable. Quite often, the free webinars provide general information which ignites other ideas for developing your niche. Seminars and conferences occur throughout the year at different times and locations that focus on all fields of investigation. The option of seminars and conferences can be helpful on another level. It provides the opportunity to network and meet others face to face in your field. It is an excellent way to develop your network, learn your specialty and create new clients. Most states within the US have state associations for licensed investigators. This is another option to connect with and create an extended network / clientele.

It is best to work from your strengths when developing your niche. Determine those strengths and develop through training, networking and experience. The specialty you develop will help to create a stronger and more powerful business.

ISPLA Update
Bruce Hulme

NEW YORKGPS TRACKING --
This past Wednesday in a 3-2 decision, the Appellate Division, Third Department ruled that the New York State Department of Labor was within its rights when it utilized GPS tracking to follow an employee during and after work hours and while on vacation with his family.

It dismissed the claims of Michael Cunningham, a former Labor Department employee, that the use of a GPS tracking device constituted an illegal search and seizure. Last year, the department fired Cunningham (who was first hired in 1980) for misconduct, relying on GPS data to show that he had submitted false expense sheets and other travel records. Cunningham sued, claiming the data should have been suppressed at his termination hearing. He demanded a new hearing but not reinstatement.

As reported by Thomson-Reuters, the court ruled that because the device was only monitored by an investigator during work hours, its use was constitutional. "To establish a pattern of serious misconduct, it was necessary to obtain pertinent and credible information over a period of time," Justice John Lahtinen wrote for the majority. In his dissent, Justice Edward Spain argued that while the use of a GPS device to track employees suspected of misconduct is reasonable during work hours, the scope of the use in Cunningham's case -- which included tracking him during a week-long family vacation -- was unconstitutional. "(The Labor Department's) valid interest in (Cunningham's) whereabouts extended only to the hours of his workday, yet the device placed on (his) personal vehicle collected data 24 hours a day, seven days a week," Spain wrote.

Since the decision was split, Cunningham may appeal to the Court of Appeals, New York's highest court, without permission from the Third Department. He was represented by Corey Stoughton of the New York ACLU. The New York Attorney General's office represented the NYS Department of Labor. The case is Michael Cunningham v. New York State Department of Labor, New York Supreme Court, Appellate Division, Third Department No. 512036.
http://blogs.wsj.com/digits/2011/11/23/new-york-court-state-gps-tracking-of-worker-was-justified/?mod=google_news_blog

2703 ORDERS - ELECTRONIC COMMUNICATIONS & PRIVACY ACT --
Icelandic parliamentarian Birgitta Jonsdottir, researcher Jacob Appelbaum and Rop Gongrip, an encryption specialist, have been fighting a grand jury's efforts to gain access to their information in an investigation of WikiLeaks' release of a classified military video of a helicopter firing on civilians and journalists. The court's decision ruled the foregoing three WikiLeakers had no reasonable expectation of privacy in their use of Twitter, as they had agreed to Twitter's privacy policy, thus allowing law enforcement authorities access a user's IP address.

They had argued that no one reads those privacy policies (which at least one study has demonstrated). But the recent ruling throws out that argument, stating that "petitioners' apparent willingness to provide their information to Twitter undefined with or without reading Twitter's policies undefined weighs in favor of finding that petitioners voluntarily

revealed their IP address information to Twitter."

"Even as the court set anti-privacy precedents for individuals online, it also provided more support for the secrecy of law enforcement's requests for users' Internet data, known as 2703 orders under the Electronic Communications and Privacy Act. The WikiLeakers had hoped to unseal more documents that show what data the grand jury has requested from Internet services they use–a report by the Wall Street Journal last month indicated that Google received a similar order to reveal data–but the judge ruled that nothing more would be unsealed, and made an argument against unsealing 2703 orders in general."
"Allowing routine challenges of 2703 orders would undermine grand jury secrecy, which helps maintain the integrity of the grand jury's function," the ruling states, arguing that electronic data in particular can be erased if a subject of an investigation learns of the data request. "Surprise in the execution of a 2703 order may therefore be even more important than speed." It went on to quote a Supreme Court ruling: "Although many governmental processes operate best under public scrutiny, it takes little imagination to recognize there are some kinds of government operations that would be totally frustrated if conducted openly." Though the court may have only been addressing the status of 2703 orders, that's a statement that also sounds like a rebuke of WikiLeaks' mission itself.
Link to Court ruling furnished by Wired:
http://www.wired.com/images_blogs/threatlevel/2011/11/twitter_wikileaks_ruling.pdf

NATIONAL COUNTERINTELLIGENCE REPORT --
The Office of the National Counterintelligence Executive has released its 31-page "October 2011 Report to Congress: Foreign Economic Collection and Industrial Espionage," regarding foreign spies stealing U.S. economic secrets in cyberspace. The report concentrates on China, Russia, and some friendly states as the prime culprits.
http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Federal Court Orders Assets Seized from "Troll" Righthaven, LLC -- U.S. District Court Judge Phillip Pro ordered U.S. Marshals to seize $64,045.60 from Righthaven, LLC, a law firm which failed to pay the defendant a judgment on a copyright infringement case it lost in Las Vegas. It includes $30,000 for the defendant Wayne Hoehn's legal fees in successfully asserting fair use of material posted to a website. Righthaven specializes in copyright law, and since March this year filed 275 lawsuits against websites that might be posting content without authorization belonging to the Las Vegas Review-Journal or The Denver Post. The law firm, having purchased rights to articles published by both newspapers, sued bloggers for infringement and then lost a number of suits when "standing and fair-use defenses were successfully asserted," according to an ABA Journal article.

Hoehn's attorneys argued that the lawsuit infringed upon his rights to free speech. Righthaven argued that Hoehn had posted a Review-Journal story online without permission. If the collection of the judgment is successful, the Randazza Legal Group of Las Vegaswill get the money, for representing Hoehn. However, Righthaven, may appeal the dismissal of its suit against Hoehn and the attorney's fees award to the 9th U.S. Circuit Court of Appeals, claiming that it might go bankrupt should it be required to pay the $64,000.

STATE ASSOCIATIONS FINANCIALLY SUPPORT ISPLA --
ISPLA is grateful to the professional associations that have acknowledged our legislative efforts at the federal level these past three years. Recent state association contributions have included $1000 from the New Jersey Licensed Private Investigators Association, $2000 from the Pennsylvania Association of Licensed Investigators, $2500 from the

Associated Licensed Detectives of New York State, and an additional $2500 from that association's Security Guard Company Committee. It is through the support of associations such as these and of our individual members that we are able to finance our state and federal legislative tracking systems, maintain FEC compliance of our political action committee, and professionally execute the effective Washington lobbying campaign of our volunteers and achieve continuing successful results.

Thank you!
Bruce Hulme
ISPLA Director of Government Affairs
To join us and support our good work --
Please go to: www.ISPLA.org

Digital Forensics: Current Practice and Application in the Private Sector

Randall L. Weston
Charles W. Rettstadt
Research North Inc.
Petoskey, Michigan

Executive Summary

Staying current with changes in digital technology has become a daunting task for the computer/mobile phone forensic examiner. Given the increasing number and variety of devices and their associated uses, it is even more of a challenge for investigators working with counsel to ensure that evidence is gathered legally. This article describes current examination and evidence handling protocols and cites specific applications to the civil arena.

Challenges to the Examiner and the Professional Investigator

It's hard to imagine what a day would be like without personal computers or the Internet! According to the United States Census Bureau (2011), in 1984 only 8.2% of American households had personal computers. Most recent data (2009) found that 68.7% now have Internet access while multiple computers and home wireless networks are commonplace.

Computer and mobile phone technology has become integral to our everyday lives; connectivity is an imperative not an alternative, and access is available to the poorest Americans, as well as the rich. Daily activities include: voice, texting, e-mail, practical Internet applications such as electronic bill paying/banking, online games and gaming activities, casual and formal communicating via social media sites and all types of formal and casual research. There are also a myriad of phone applications that involve the use of search engines to check the stock market, news and weather and to research products and services. Application of this technology has accelerated so rapidly with the advent of the cell phone that the PC and the laptop are rapidly losing popularity and being replaced by smaller, more portable and powerful devices.

Apple has set several one day sales records on the recently introduced iPhone 4 with daily sales exceeding 223,000 units per day. Add in 9.25M IPads sold, and sales jump to 325,000 iOS (mobile operating system) devices per day.(1) Samsung and Research in Motion (Blackberry) have also introduced new tablet computers while strong sales continue for all of the Smartphones.

Total mobile phone sales to end users in 2010 totaled 1.6 billion units, an increase of 31.8 percent from the year 2009. It is now estimated that 90 percent of Americans own some type of mobile phone.(2) The popularity of tablet devices has contributed to a significant decline in sales of traditional netbooks, laptops and desktop PCs. A tablet or a Smartphone is certainly more personal since both work-related and personal content can be stored in these hand-held devices. They are capable of accessing high-speed Internet via cellular service, and Wi-Fi hot spots are commonplace. They can be used virtually anywhere.

Best Practices for the Examiner

With the rapid change in technology and the limited training available on new devices, it is important for an examiner to remain current in his/her knowledge of acceptable research tools and methodology. Tools need to be tested and validated prior to each use and established best practices for computer forensic examination must be followed.(3)

To extract information from any device, an examiner must first determine what information is potentially available on the subject make and model. Smartphones are particularly challenging since not so long ago all cell phones had only a rudimentary call history, phone book, and a messaging system containing both voice and text messages. Today's devices are much more complex, some with operating systems similar to that of a laptop.

The most common question asked of examiners is "What potentially probative information can be forensically extracted from a device?" The answer is, "Some or all of the following depending on the manufacturer, make, and model":

- Installed applications
- Phone book/contacts
- Recently dialed numbers
- Call logs
- Text messages
- SMS messages
- MMS messages (Media Messages)
- Memos
- Browsing history
- E-mails
- Audio and video recordings
- Pictures
- Appointment calendar entries
- GPS data (locations the phone has been)
- GPS location of photos taken
- Hot list
- Pin data
- SIM card data
- Data stored on internal and removable memory
- Service provider
- IMSI
- Spyware artifacts
- Other hidden data

Collecting and protecting data is accomplished by an examiner utilizing a tiered approach. Multiple tools and methods are employed to examine and extract all available data from an enormous variety of mobile and stationary devices. As a result, the consensus is that, "More forensically sound levels should be exhausted before attempting a lower level of analysis."(5) This is accomplished utilizing forensic procedures in the following order:

- Forensic cellular/handheld device software
- Consumer (open source and/or manufacturer's) backup software
- Menu navigation, photographic/video documentation and transcription of information viewed
- Transfer via e-mail or messaging of data to a downloadable device

After evidence extraction is completed, final steps include preservation and reporting of methodology and findings. Whether for criminal or civil proceedings, the report should contain all relevant case information and detail the procedures followed during the forensic examination process.

Documentation should include:

- Copy or description of legal authority
- Chain of custody
- Detailed description of the evidence (may include photos)
- Photographs or documentation of any visible damage
- Information regarding the packaging and condition of the evidence upon receipt by the Examiner.

Best Practices for the Professional Investigator

Prior to presenting any device to a forensic examiner, the following should be considered to preserve evidence in its original state:

1. Is the device currently powered on or off? If it is on, is it connected to a network and available to receive data? There are applications that provide remote access to phones such as Apple's "MobileMe", which allow a subscriber to remotely wipe the contents of a phone. Other applications enable a device to be tracked by GPS in the event it is lost or stolen. Finally, if left on, the contents of a phone can also be impacted by incoming data. For instance, most cell phone manufacturers utilize the "first in-last out" principle for data. This means any incoming data will replace or delete existing data such as text messages, phone call logs, etc.

To avoid unwanted/unintended corruption or manipulation of data, a device should be turned off. If the device is a cell phone, this will preserve the integrity of the data and location of the last cell tower accessed.(4) If a device must remain on, it should be isolated from all network access by using a Faraday Bag or a similar piece of hardware that provides radio frequency shielding. It should also be connected to a charger and the examiner notified for immediate forensic examination.

2. Some data may be lost when a phone is powered off, and powering off without knowledge of the device's password can add a complication. Accessing password protected devices can be very labor intensive, and special software or the pin code from the manufacturer may be required.

Civil Applications

Traditional abuses of digital devices have included criminal and civil infractions related to adult and child pornography, Internet and electronic mail misuse, fraud, forgery and counterfeiting, marital infidelity (chat logs, Internet history, e-mail, and text messages), identity theft and sexual harassment to name a few. In the past, law breakers communicated their illegal acts verbally and in writing. Today, these acts are routinely communicated digitally.

Recent, more novel abuses of digital devices have presented huge challenges to the business community. For instance, the authors recently received a complaint from a manufacturing company's human resource director that a female employee had been receiving sexually explicit messages on her cell phone, and the sending number was blocked. An investigation identified a male employee as the potential sender. As part of the investigation and under the guise of an upgrade, the employer exchanged that employee's

assigned company-owned phone. A forensic examination provided the proof that the suspected male employee had sent the offending messages. As a result, the manufacturing company was able to prevent a potentially costly sexual harassment lawsuit.

Business information technology departments are tasked with monitoring the use and abuse of company systems. In another case investigated by the authors, a large health care institution's IT manager requested assistance with a suspected Health Insurance Portability and Accountability Act (HIPAA) violation. The IT department had discovered that patient information including social security, insurance and diagnostic data had been sent to an employee's personal e-mail account. Investigators also sought to determine if the protected information was used or transmitted from the employee's company-assigned computer. A forensic examination of that company-owned laptop determined that the protected information was intact and that none of the patient's confidential information had been compromised. This investigation developed the proofs necessary for the health care institution to remain in compliance with the HIPAA Security Rule. (6)

Conclusion

Rapid changes in the diversity and complexity of digital devices present increasing challenges to prosecutors, attorneys, forensic examiners, police and professional investigators. Everyone involved in the process must remain current on examination practices and protocols as well as legally acceptable methods of obtaining and preserving of evidence.

There are no short cuts! Best practice demands that examiners, police and investigators should vigilantly avoid intrusive behavior where there is a reasonable expectation of privacy, should remain current on legal precedent and should maintain a close working relationship with prosecutor or counsel throughout the investigation.

Footnotes

1. http:/techcrunch.com/2011/07/19/apple-smashes-through-iphone-sales-records-0nce-again-sold-20-34m-last-quarter/
2. Wikipedia.org/wiki/Mobile_phone#Mobile_phones_in_society
3. Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Mobile Phone Examinations. Version 2.1 (July, 2006)
4. Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Computer Forensics Version 1.0 (July 2009)
5. Scientific Working Group on Digital Evidence (SWDGE) document released May 21, 2009
6. www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

About the Authors

Randall L. Weston has over 20 years of experience in law enforcement as a Lieutenant with the Department of Public Safety, Petoskey, Michigan. Randy is responsible for supervising and conducting criminal investigations, specializing in those involving the Internet, computers and cell phones. He is a Certified Digital Evidence Technician and is recognized in Michigan courts as qualified in computer-related evidence gathering and computer forensic investigations. Randy investigates civil matters as an employee of Research North, Inc. with permission from his Department.

Charles W. Rettstadt, a member of Intellenet, is a former Naval Criminal Investigator, and for 10 years worked as a Special Agent for the Michigan Attorney General, Organized Crime Division investigating white collar crime. More recently, he has been President of Research North, Inc., a well-respected Midwestern private detective agency serving the insurance industry and the business community. Charlie has an MA in Police and Public Administration, is a Certified Fraud Examiner and has been qualified as an expert in fraud schemes and financial transactions.

Stalking Intervention

Tanya S. DeGenova
TSG Security Consulting, Inc.
Boston, Massachusetts

Stalking is a term commonly used to refer to unwanted and obsessive attention by an individual or group to another person. Stalking behaviors are related to harassment, abuse and intimidation. According to Dr.Sam Vahnin, who wrote *Coping with Various Types of Stalkers*, the stalker may be using Emotional, Verbal, and Psychological Abuse, Domestic and Family Violence and Spousal Abuse. The stalker may be following the victim in person and/or monitoring them via the Internet.

While the criminal penalties for stalking vary from state to state and depend on the degree and means of stalking and whether the stalking occurred as a result of a violation of a restraining order, all states in the U.S. agree on a strong punishment for stalking, which ranges from one to five years in prison and is normally accompanied by a fine ranging between $1,000 fine and $5,000.

For example, in the Commonwealth of Massachusetts, two existing state laws protect victims from stalking through unwanted annoyance and/or as result of violation of a restraining order:

ALM GL Ch. 265, § 43. Stalking. (1997)

(a) Whoever (1) willfully and maliciously engages in a knowing pattern of conduct or series of acts over a period of time directed at a specific person which seriously alarms or annoys that person and would cause a reasonable person to suffer substantial emotional distress, and (2) makes a threat with the intent to place the person in imminent fear of death or bodily injury, shall be guilty of the crime of stalking and shall be punished by imprisonment in the state prison for not more than five years or by a fine of not more than one thousand dollars, or imprisonment in the house of correction for not more than two and one-half years or both. Such conduct, acts or threats described in this paragraph shall include, but not be limited to, conduct, acts or threats conducted by mail or by use of a telephonic or telecommunication device including, but not limited to, electronic mail, internet communications and facsimile communications.

(b) Whoever commits the crime of stalking in violation of a temporary or permanent vacate, restraining, or no-contact order or judgment issued pursuant to sections eighteen, thirty-four B, or thirty-four C of chapter two hundred and eight; or section thirty-two of chapter two hundred and nine; or sections three, four, or five of chapter two hundred and nine A; or sections fifteen or twenty of chapter two hundred and nine C or a protection order issued by another jurisdiction; or a temporary restraining order or preliminary or permanent injunction issued by the superior court, shall be punished by imprisonment in a jail or the state prison for not less than one year and not more than five years. No sentence imposed under the provisions of this subsection shall be less than a mandatory minimum term of imprisonment of one year for a first time offense.

Furthermore, in the Commonwealth of Massachusetts, the punishment is even stronger for a second or subsequent stalking offense. The law reads:

(c) Whoever, after having been convicted of the crime of stalking, commits a second or subsequent such crime shall be punished by imprisonment in a jail or the state prison for not less than two years and not more than ten years. No sentence imposed under the provisions of this subsection shall be less than a mandatory minimum term of imprisonment of two years.

Whatever means the stalker is utilizing in annoying or threatening the victim whether the threat is physical or emotional, a stalking complaint always warrants a swift intervention.

Just as an employee acting in a threatening matter in the workplace poses a threat to the employees, a stalker poses a real threat to his/her victim, as in both cases, the aggressor(s) are exhibiting emotional instability and their impulsive behavior has the potential to escalate into an act of violence. Therefore, immediate intervention is necessary to fully assess and deter the threat and protect the victim(s).

Case study:

I was recently contacted by the parents of a Boston co-ed (victim/client) who is being stalked by a former boyfriend.

After a short-lived consensual summer romance in Cape Cod, MA, with a man over twenty-years older than her, the co-ed became concerned by the man's manipulative, over-emotional behavior, his heavy drinking and erratic driving. She tried to break off the relationship, when she returned to college telling him "it is not going to work out."

Throughout the month of September, the man ("stalker") continued to send multiple daily text and e-mails in which he begged her to see him again, and continued to leave her emotionally charged voicemails, often crying on the phone.
Over Columbus Day weekend, in mid-October, the co-ed returned to the gallery on Cape Cod where she had worked over the summer, without telling the man in question. On her last day on the Cape, as she was closing the gallery, the man appeared unannounced on the steps of the gallery and begged her to talk to him. When she refused and walked passed him and got into her car, he began calling her repeatedly threatening to make a scene in front of her parents country club in the little seaside town, if she did not agree to come talk to him. She finally gave in and drove to the country club to have a chat with him. The man began crying, begging her to resume their relationship. She asked him to leave her alone and to please stop calling her, but that did not stop his persistence.

For the next week or so, he continued calling her several times per day, in addition to sending her text messages and emails. This unwanted attention was becoming very annoying and disruptive to her and to her studies and prompted her to block the man's cellphone number. While this brought some relief to her, the emails kept coming steadily and now, there were also love letters sent to her dorm. Her annoyance began to turn to anxiety. She finally replied to one of his emails and asked him again to stop contacting her; otherwise, she would bring her father into this matter.

The situation came to a head, when about a week ago, at 10 p.m., as she was coming out of her classes, she saw the man standing on the sidewalk of her college campus in Boston, waiving to her hello. She walked right past him without acknowledging his presence or making eye contact with him. When she returned to her dorm that night, some distance away, she found two new emails from him, in which he complained that she didn't stop to say hello to him and explained that he had just moved to her Boston neighborhood. He wrote that he was staying at a cousin's house (of whom he never spoke about to her in the past) and that he was planning to open a business in Boston. He warned her that they might occasionally run into each other from time to time and that there was no need for her to ignore him.

This was the straw, which broke the camel's back. The co-ed never even heard of the man having a cousin in Boston and especially so close to her campus. Her anxiety now grew stronger. While she had never invited the man up to her dorm and never told him where her parents lived, she did have him pick her up by her dorm once, back in September when they were still dating, and allowed him to walk her to her classes. Having now received mail from him at her dorm and having seen him on her campus, precisely when she came out of her classes late at night, convinced her that he was stalking her.

When the co-ed's father learned of the situation, he immediately searched the man's name in "Google" and discovered that this man was recently charged with his fourth DUI (Driving under the Influence) on Cape Cod. This is when the father contacted me asking for help. The father wanted some immediate

intervention, but didn't want to spend too much money, as he read in the newspapers, that a fourth DUI offense normally carries a minimum of two years incarceration. The father therefore presumed that the man will go to jail soon and that will resolved the "unwanted suitor" for his daughter.

We immediately sat down with the co-ed and conducted an in depth interview of her past relationship with this man. We reviewed all correspondence she had kept from him (to include all text messages, emails and love letters), screening those for any expressed threats (either homicidal or suicidal), and for any information, which would give us a window into the man's emotional stability and propensity for violence. We also looked for any additional information, which may allow us to assess the man's emotional state and his propensity for violence. We subsequently conducted a preliminary background investigation on him. Our inquiry determined that the man had a long history of alcohol/drug abuse, DUIs and reckless driving, for which he had not served any substantial time in jail. He also had a history of changing license plates on his car on a yearly basis, since his previous DUI in 2001.

Stemming from the behavior he had exhibited with this co-ed and the correspondence he had sent to her, it became clear to us, that the stalker suffers from emotional instability. While his "stalking" did not put his victim in immediate danger at present, and his behavior didn't rise to the level required to obtain a restraining order, his persistent and unwanted texting, emailing and telephone calling, if not just disruptive, were becoming threatening to our victim/client.

Furthermore, the stalker's past history suggested that there was a very strong chance that he might not be sentenced for his fourth DUI until several months from now and that he may not serve the two-year mandatory sentence prescribed for such an office under Massachusetts Law. Moreover, and despite the fact that his Massachusetts's driver's license had recently been revoked for a period of five years, upon his arrest, there was a strong chance that he may continue driving from Cape Cod into Boston using different plates.

We therefore put a package together for Campus Police, which included the man's picture with full description of his vehicle, his behavior and past driving history. We also provided the Director of Campus Security the co-ed's full identity, address and cellphone number. The Director of Security, at Campus Police of the college she attends, in turn and per our request, assigned a point of contact (POC) for her to call, when she needs an escort at night when she walks back to the dorm from classes alone, or for her to call in an event of an emergency.

The co-ed felt reassured, whereas her parents were relieved with the outcome and please with our response/intervention. The parents decided to expand our engagement to continue to monitor any correspondence their daughter may receive from this "stalker" (both via email, or snail mail). We also instructed the co-ed to document all contacts or sightings of the man in her neighborhood or on campus, report any such contact to us and immediately contact campus police to ensure her safety and to create a record. If in fact the "stalker" continued to harass her that would demonstrate the "next step" in his stalking activity and could serve as grounds for us to help her apply for a restraining order against him.

Whatever your client's stalking circumstance may be, as a private investigator/security consultant retained in this case, you must intervene swiftly and immediately conduct a threat assessment via a thorough interview of the victim to determine the stalker's state of mind, his/her history of violence, noting any erratic/impulsive behaviors, any criminal history, including, but not limited to driving history and any history listed on the sex offender's registries. You should also look into the stalker's motive for pursuing the victim and measure his/her potential (whether homicidal or suicidal) as well as his/her access to weapons.

If your preliminary investigation determines that there is no imminent danger to your victim, or that the threat posed by the stalker doesn't meet the threshold required for obtaining a restraining order, but that the stalker demonstrates either emotional instability of, has a criminal history, or ability to access

weapons, the incident should be immediately reported to the nearest law enforcement agency (campus police, security department or local police department).

Additionally, should the situation escalate to the point, where the safety of the victim merits a restraining order and/or leads to prosecution, documentation of the stalker's persisted and unwanted attention will be key in building a case. The security consultant/investigator, in concert with the victim, must document, document, document.

It is imperative to keep a log of the stalkers telephone calls and of any encounters with the stalker, including dates, times, and witnesses to these encounters. The main thing is to call the police when things happen (no matter how minor they may seem to be at the time) and to document everything. Building a stalking case is very much like putting together a jigsaw puzzle. In the end, all pieces of the puzzle will fit together, hopefully before a serious act of violence occurs.

Finally, a credible complaint concerning persistent and unwanted attention from an old boyfriend and /or ex-husband, often rated as a very low priority for a busy police department must be taken seriously by a private investigator/security consultant, as more often than not, threat(s) escalate into acts of violence and an "unwanted attraction" can quickly turn into a "fatal attraction".

Tanya S. DeGenova, a member of Intellenet, is a retired FBI Special Agent where she served in various supervisory and management positions. Ms. DeGenova is a licensed private detective in Massachusetts and has served on the Board of Directors of the Licensed Private Detective Association of Massachusetts. She is active in many civic organization in the Boston area.