INTELLENET *News*

Official Newsletter of the International Intelligence Network, Ltd.

Intellenetwork.org *Summer 2016*

In this issue...

Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet

Dear Intellenet Members:
In August Intellenet will be at the World Investigators Conference …

I hope your summer is going well. We are now past our successful Toronto, Canada conference. As you could see from the many posts on our listserv after the conference everyone had a great time. No conference can be successful without the help of many, thank you to all those that helped. In particular I want to thank George Michael Newman, Robert Dudash, Ed Spicer, Jeff Stein and of course Jim Carino for helping make the conference such a success. Planning for our 2017 conference in Denver, CO is well underway. We will be providing dates and hotel information in the coming weeks.

"… we will also be exhibiting at the LPDAM conference this September. This continues our recruitment efforts which have been working very well over the past few years."

In August Intellenet will have a booth at the 2016 World Investigator conference being held outside of Huston, TX. We will also be exhibiting at the LPDAM conference this September in Natick, MA. This continues our recruitment efforts which have been working very well over the past few years. I encourage members to stop by the booth and say hello. These conferences are great opportunities for networking and learning, but also present an opportunity for members to recruit for our association. Do not hesitate to bring a prospective member by the booth to have their questions answered and to find out more on why Intellenet is the premier investigation association worldwide. Remember that we are the only association that has a 10 year minimum investigation experience requirement as well as full background checks on all applicants.

I am pleased to announce that we have begun our "security business initiative." In furtherance of this project, two specific programs have been initiated.:

1) For those who have an interest in security consulting as an additional business opportunity, a subject specific listserv—IntellenetSBI—has been developed to facilitate transfer of information about members. The back end of the listserv will also contain several documents that can be used by individuals. Please contact Bill Blake or Jim Carino if you are interested in being included on this listserv.

2) A security consulting workshop, *"Increasing Your Business Opportunities—Become a Security Consultant,"* will be held at the CSI Academy of Florida in Alachua, FL (Gainesville area) on January 12-13, 2017 which will include specific information on what are significant areas for preventing negligent security litigation and how to "sell" this product to clients.

I look forward to seeing many of you at the conferences we will be exhibiting at in the coming months. For those that I don't get a chance to see, I hope the rest of your summer is a great one.

As always, you can reach me by phone at (734) 320-9240, or by email at peter@ewiassociates.com.

♦♦♦

Member News

Welcome New Members !

Bill BUZZELL — Hamilton (Missoula), MT
Joe CICINI — Miami, FL
Ryan COLLEY — Washington, DC / Columbus, OH
Jennifer KIESELING — Frenchtown, NJ
Sachit KUMAR — New Delhi, India
Seldon (Don) NASON — Concord, NH

These are our new members since we last published. Peter featured each in an InfoBrief. When you need "intel" in these locations, you now know where to turn. You can update your membership listings on the web and in the Briefcase Roster, by sending info to intellenet@intellenetwork.org.

"Featured Speaker — Sean Mulholland, CFE ..."

Sean recently presented a two hour seminar on "Cyber-Fraud" to the Florida Institute of Certified Public Accountants in Orange Park, Florida. In August he will be presenting: "Social Media As Evidence" to the International Association of Special Investigative Units in Ft Lauderdale. Sean was selected to be part of the 2016-17 Class of ***Leadership Jacksonville***. Further congratulations are in order for Mulholland Investigation & Computer Forensics, which celebrates its twentieth anniversary in August.

The Korean Risk Landscape ...

Intellenet member **Rodney J. Johnson** of Erudite Risk sends a reminder that Erudite's Korean Risk Intelligence subscription is available to Intellenet members free of charge. Their report covers the Korean / Asian risk landscape, "... *looking at your own markets for opportunities with new eyes and for interacting with your own clients.*" To receive the reports, contact Rodney at rodney.johnson@eruditerisk.com.

eruditerisk KOREA RISK INTELLIGENCE

"Featured Speaker — Kitty Hailey, CLI ..."

Philadelphia's own **Kitty Hailey, CLI** will be featured at three (3) events in September. She will be a part of a PALI panel on September 12-13, 2016 in Hershey, PA. and a speaker at the LPDAM conference in Boston, MA September 16-17, 2016. Then it's to Florida as a speaker at the FAPI conference in Tampa, September 21-24, 2016. It's a busy travel month for Kitty, talking on ethics and introducing the third edition of her popular book, *"Code of Professional Conduct: Standards and Ethics for the Investigative Profession."*

Congratulations, Nasr ...

Nasr Al Homoud is the newest Intellenet board member. Nasr is in Guatemala City. His firm provides security consulting services and executive protection. Fluent in Spanish and Arabic, he can be reached at nzrhmx@gmail.com.

Member News continues on next page ...

LPDAM's 25th Anniversary Celebration & Conference

Intellenet member and Licensed Private Detectives of Massachusetts (LPDAM) President **William Connors** is proud to announce that the LPDAM will hold its 25th Anniversary Celebration & Conference on September 16-17, 2016 at the Hampton Inn Conference Center, 319 Speen St., Natick, MA. The conference program features two days devoted to educating private investigators, law enforcement, attorneys, paralegals, investigative reporters, and those wishing to learn more about investigations. The conference will feature a collection of talented local and national speakers. We traditionally anticipate between 100 and 150 attendees for this event. Each participant is a professional who devotes a major portion of his or her practice and business to investigative matters.

Confirmed sponsors as of this time are: **Intellenet,** PI Magazine and the Campbell Group. Speakers subject to final confirmation include: Intellenet members **Kitty Haley, Jeff Stein, Jimmie Mesis** and **Bruce Hulme**; Rick McMaster, Fox TV25 investigative reporter Bob Ward, Attorney Steve Lander, John Hoda and Attorney Eric Osterberg.

Hotel room rates for this event have been deeply discounted at $119.00 per night. This rate will be available until August 30, 2016. For overnight accommodations, please call the Hampton Inn at 508-653-5000 (mention the LPDAM Conference).

For more information check out www.lpdam.org.

•••

The Florida Association of Private Investigators (FAPI) has announced that their annual training and litigation seminar will be held Sept. 21-25 at the Hilton Hotel in Altamonte Springs, Florida. The theme of this year's conference is International Investigations. To that end, **Harvey Morse** (Chair), is bringing in guest speakers from Asia, Mexico, Canada, the Middle East, South America and other locations regarding what can and cannot be done by the private sector in those geographical areas. There will also be training in medical investigations, an ethics course and other events. **Harvey** is pleased to announce that the Keynote Speaker this year will be **Chief Jarrod Burguan**, of the San Bernardino Police Department (seen here), who will address the attendees on the terrorist attack in his city. Reservations can be made now at: www.myfapi.org. Typically, many **Intelleneter's** and **BAI's** are in attendance!

Member News continues on next page ...

Captain Eileen Law …

Not only is **Eileen** a licensed Captain with the Coast Guard, but a Vice Commodore of her yacht club, part of the Yacht Clubs of Maryland. She recently served as Northern Chesapeake Bay Liaison for the "Wounded Warriors Day on the Bay " Project. Here's a note from Eileen on this special event …

"Each year, 75 captains from New Jersey to Virginia take 75 wounded warriors along with their families out on our yachts for a day of cruising on the Chesapeake Bay … We give them duffel bags and back packs filled to the brim with gifts … gift cards, a day at the spa for their spouses, movie theatre tickets, shirts and more. We buy things for their children … At the end of the day, we have a huge picnic … By the way, we are a whole separate entity from the Wounded Warrior Project. We are all volunteers …"

Intellenet Members Speaking at the 2016 WIC

Among the impressive lineup of speakers in August at the World Investigators Conference at La Torretta Lake Resort in Texas are several Intellenet members: **Fernando Fernandez, Mark Gillespie, Harriet Gold, Paul Jaeb, Kelly Riddle** and **Allen Stidger.** Intellenet is an exhibitor. The conference is produced in concert with TALI and members **Jimmie** and **Rosemarie Mesis.** Jimmie is presenting a pre-conference seminar, "How to Build & Double Your Agency Income." The conference also features a golf tournament and handgun shooting competition. It's not too late to register. Details at 2016wic.com.

♦♦♦

Intellenet Member Kevin McClain Announces ...

READI™ RESPONSE

Get READI to Jumpstart Your Business!!

The READI Response Team is Looking for Intellenet Partners Nationwide

Join the only nationwide network of professional investigators that will be offering a rapid response to major incidents (accidents, slip /trip and falls, and risk management related issues) through a nationwide network of investigators connected through the patented pending technology of the **READI** Response Mobile App! Clients are ready to join the network we need investigators to be **READI!**

With your affiliation in Intellenet the most prestigious intelligence association in the world you are granted waiver from the fees for training, vetting and background requirements.

Successful candidates / agencies must possess the following:

- Excellent communication, both written and verbal, trial testimony experience is a plus;
- Excellent computer, smart phone and organizational skills with the ability to work independently;
- Flexible in work schedules, availability and willingness to accept assignments on a rush basis;
- Ability to work nights, weekends and holidays. When incidents happen we are first with boots on the ground;
- All candidates must have fully insured vehicle, proof of liability insurance, and proof of investigator license (states that require). Smartphone (I-Phone or Android) or I-Pad or Tablet compatible with operating system;
- We are also looking for specialist in accident reconstruction, security premise negligence, slip/trip and falls, claims, risk management, OSINT / internet / social media research, surveillance, executive protection, workplace violence, and background investigations.

THIS REVOLUTIONARY NEW CONCEPT IN INVESTIGATIONS IS SET TO LAUNCH SUMMER 2016!!

THE FIRST 500 INVESTIGATORS WHO SIGN UP WILL RECEIVE A ONE YEAR COMPLIMENTARY TRIAL SUBSCRIPTION.

Call 877-532-1152, email: readiresponse@gmail.com or visit: www.readireponseteam.com.

♦♦♦

Recruitment Needs USA

ALABAMA	Southeast Corner (Dothan), Auburn, Mobile
ALASKA	Fairbanks, Nome, Anchorage
ARKANSAS	Blythville area, Jonesboro area, Springdale
CALIFORNIA	Redding
COLORADO	Colorado Springs, Pueblo
FLORIDA	Key West
GEORGIA	Brunswick, Macon, Savannah, Valdosta
IDAHO	Idaho Falls/Pocatello, Mountain Home area, Twin Falls
ILLINOIS	Peoria, Urbana/Champagne, extreme southern top (Cairo area)
IOWA	Sioux City, Davenport, Waverly (we have Cedar Rapids and Monroe City covered)
KANSAS	New Colby, West/Dodge City, Anywhere in west part of state
KENTUCKY	Bowling Green/Hopkinsville (SW) and SE
MAINE	Bangor, North
MARYLAND	Cumberland
MICHIGAN	Midland/Bay City/Saginaw
MINNESOTA	Duluth, International Falls, Moorhead
MISSISSIPPI	Biloxi, Greenville, Hattiesburg, Tupelo
MISSOURI	NE, NW, SE (We have Springfield, St. Louis)
MONTANA	Great Falls, Kalispell
NEBRASKA	North Platte, Scottsbluff (We have coverage only in Omaha and Lincoln)
NEVADA	Carson City, Elko
NEW MEXICO	Roswell/Clovis, Santa Fe (We have coverage only in Albuquerque and Las Cruces)
NORTH CAROLINA	Kinston – New Bern area, Outer Banks area

Continued on next page ...

Continued from previous page ...

NORTH DAKOTA	Bismarck, Minot
OHIO	SE area
OKLAHOMA	SE, Guymon area (We have coverage only in Oklahoma City and Tulsa)
OREGON	La Grande/Pendleton, SE
SOUTH CAROLINA	Greenville/Spartanburg, Myrtle Beach
SOUTH DAKOTA	Aberdeen, Pierre, Sioux Falls
TENNESSEE	NW
TEXAS	Beaumont, El Paso, Galveston
UTAH	SE area
VERMONT	Rutland/Southern VT
VIRGINIA	Fredericksburg, Norfolk, Newport News, Roanoke
WASHINGTON	Bellingham
WISCONSIN	Wausau, Eau Claire
WEST VIRGINIA	Clarksburg/Fairmont/Morgantown (1 of 3)
WYOMING	Caspar

Footnotes:

1. Except for AK and HI a goal is to have no location more than a two hours drive for our nearest physically located member. Members are requested to check individual states/countries to increase coverage effectiveness.
2. The ETS contract suggests one hour drive time for our nearest physically located member is best case in contiguous 48 states.
3. Many of the above areas can be covered by members on an On Call basis. Check the Briefcase Roster.

On Call areas are not cost efficient to clients but do increase our investigative assistance/effectiveness.

This list was published in July when Peter sent an email to the listserve with the Recruitment Needs attached. If you have a candidate recommendation for coverage in one of these locations, please contact Peter.

A Story

by

Harvey Morse

I had the pleasure of meeting **Maurice Hicks** and his wife, **Kim,** for the first time when they hosted the Las Vegas Intellenet meeting, and we have maintained a relationship ever since. Unbeknown to Maurice at the time, I had a friend in Vegas who was a very popular entertainer, guitar player, singer and comedian. I first met him about 35 years ago in Orlando, and enjoyed his dry wit, comedy with song, with never an off-color word. My friend's name was "**Wild Bill Cooksey**" or "**WB**" to me.

Some years ago, WB's wife was diagnosed with cancer. Having no insurance, WB and his wife, Janae, spent their entire savings on medical treatments. Unfortunately, it went on until she passed away. WB became despondent, stopped his club work and lingered in agony. One of the brightest people I have ever known was now down and out, homeless, living in a broken down van, then in parks where he was harassed by the police. WB never drank alcohol, never used drugs and never smoked a cigarette. At one time he had gone to handwriting school, graduated and did some work for the LVPD, but it was short-lived.

WB stayed in touch with me and from time to time I was honored to send him a few dollars, to help find temporary lodging, and whenever I went to LV I would buy him a nice dinner and extend my hotel for a few days so he could have a place to shower and get a good night's rest.

WB knew the end was getting close and he texted me that he was now wearing my contact info around his neck under his shirt in the event of an emergency. Shortly thereafter I got a call that he was hit by a car and the driver took off, leaving WB with serious injuries. After recovering, he began playing his guitar in front of the Bellagio hotel and took photos with visitors for minuscule tips, yet he always smiled and had a kind word. The next call came when he was robbed and beaten up for his tip jar, rendering him unable to walk for months. At this time, I assisted him in finding a flop house apartment, better than the streets, of course! I contacted Maurice, sent him some cash, gave him WB's address, and he delivered the cash to get WB through for a while.

My friend was an avid user of Facebook and had a very large following. WB had even won a Guinness record by performing on stage nonstop, longer than any other person. You can google his full name and see his photo, hear his songs on You Tube and see all the famous people he performed with.

One day I realized there were no messages from WB for a while. Others became worried. I again imposed upon Maurice to go to the apartment, where he discovered WB had died. He had no family and had asked me, informally, to handle things when he passed which I was honored to do. Again, Maurice stepped up to the plate like he was my brother. Maurice helped with the police and with two large storage sheds WB owned, which were full of old food, clothes and I hate to think what else.

Continued on next page ...

After a very lengthy process, including an ex parte hearing with a judge and the involvement of the Public Administrators office, WB was cremated almost three months from when his body was discovered, and that was around the first of July. WB's passing was a very sad thing for me. His comedy and song brought so much laughter to so many people, especially me.

Had it not been for Intellenet I would never have met Maurice and Kim. Had Maurice not been the kind, concerned and helpful human being, I don't know what I would have done. Maurice and I discussed the final cremation and he did what will bring a tear to your eye: He had Janae's ashes in his possession, while waiting for WB's. He took the ashes of both to the top of the Bellagio, and let nature join these two people together over the city they both loved. Maurice did this on July 11th, at 7:11 p.m. as a tribute. I am one lucky human being to have met Maurice, thanks to Intellenet, and he has endeared himself to me forever. Hopefully he and Kim will visit us in North Carolina. I'm getting a little teary eyed writing this, but I wanted to publicly thank this awesome human being for all that he has done.

Kim and Maurice Hicks, hosts of Intellenet's conference in Las Vegas in 2015

Thank you, Maurice.

You will need twenty million dollars (yes, that's $20,000,000.00) and a target's phone number, then you will be able to intercept any call or text made on that phone. It doesn't matter where the target phone is located, nor where you are either. This unique and expensive spy tool is being offered to governments around the world by an Israeli company, Ability, which has also announced plans to market its interceptor kit to law enforcement in the U.S. soon.

Search the internet for "Unlimited Interception System (ULIN)" and you will find recent blogs and articles on Ability and its ULIN. Forbes magazine reported the following: *"All a ULIN customer requires is the target's phone number or the IMSI (International Mobile Subscriber Identity), the unique identifier for an individual mobile device. Got those? Then boom – you can spy on a target's location, calls and texts."*

Ability was founded in 1993 by former military intelligence and communications experts. The ULIN is unique in that it does not require proximity to be effective, nor does it require the consent of the mobile carrier for the target device. The developers of the system were able to exploit a vulnerability in an international telecommunications standard relating to how networks transfer digital signals.

Stay tuned once news about ULIN hits the main stream media in the U.S. Then you will see the unlimited discussions on safety versus privacy.

♦♦♦

Chief Risk Officers needed to battle rising corporate espionage

Reprinted with permission from ***CSOonline.com***

By Bob Violino

A growing number of organizations are adding a new member to the C-suite—the chief risk officer (CRO)—and the rise of these executives is having a direct impact on the security programs at enterprises.

"Corporate espionage, terrorism and cyber attacks are ratcheting up the need for senior executives who understand all aspects of risk management and security," says Jeremy King, president of Benchmark Executive Search, a provider of technology executive search services.

"Many companies are finally awakening to how destructive security breaches of all types can be—from physical damage and real costs to reputation loss and customer recovery," King says. "Previously siloed risk-management functions must be reinvented, strengthened, and funded more aggressively. Industry must re-evaluate its approach to risk management, and success will require unprecedented cooperation from board directors and those in the C-suite."

The rise of the CRO is a trend that has yet to take off, King says. "While some forward-looking, large financial players have hired a CRO to oversee all risk, most companies have yet to follow their lead," he says. "Based on what I have gleaned from clients, advisers, and our network of security talent, public companies will increasingly empower a single leader or group to take charge of their integrated risk and security strategies."

the COO, King says, with the COO having responsibility for profit and loss and the CRO being responsible for "prevention of loss."

As s rule, CROs have been gaining power and influence within their organizations. "But with most new corporate initiatives, they do not bubble up but work top down," King says. "Therefore, boards must demand this be a major initiative."

"Corporate espionage, terrorism and cyber attacks are ratcheting up the need for senior executives who understand all aspects of risk management and security."

Jeremy King, President of Benchmark Executive Search

The role of CRO is constantly changing and evolving in order to fit the needs of the business and how it makes risk-based decisions, says Merri Beth Lavagnino, CRO at Indiana University. "A static enterprise risk management role would not be an effective one, because the world we live in is constantly changing," she says.

That's also true at DocuSign, a provider of electronic signature applications. "My team has evolved to ensure we are best equipped to manage and mitigate all aspects of risk in our business," says Tom Pageler, a former special agent with the U.S. Secret Service who is now CRO at DocuSign.

"We look at all risks holistically to include physical security, operational risk, audit, compliance, and risk/security awareness and communications in addition to information security," says Pageler, who reports to the general counsel and board of directors. "My scope includes [merger and acquisition] risk, country risk, business risk and other areas outside of traditional 'security'. As such, we run a robust Risk/Security Council where our risk registry is discussed and tracked by a team of experts and business leaders."

A confluence of factors is driving the emergence of the CRO role, as well heightening the influence of existing CROs, says Nicholas Hayes, an analyst at Forrester Research.

"Factors like greater market volatility, heightened social unrest, growing reliance on proliferating third parties, and digital disruption are just some of the external factors that make it more critical for organizations to understand and successfully navigate their risk environment—and they need someone with risk acumen and experience to do this," Hayes says.

What is still a work in progress at many organizations is how the CRO fits into the corporate security management structure.

"It is no small task for any organization to achieve consensus about what must be done, what organizational assets must be integrated into their broader risk-management mission and even a standard organizational structure to determine how the CRO, CIO, CSO and CISO fit together," King says.

"Since the reporting structure of CSOs/CISOs range from the CIO, general counsel, chief compliance officer to the CEO, it is no wonder there is confusion," King says. "A new framework needs to be created which could lead to major reporting changes."

At Black Knight Financial Services, a pro-

vider of data and analytics technology for financial services firms, the CISO and director of physical security report to CRO Peter Hill, who reports directly to the CEO as well as a risk committee of Black Knight's board of directors.

"Information security comprises a significant portion of the risk landscape of the company, and it is critical to have this function closely aligned to the overall strategic risk direction of the company," Hill says. "This reporting relationship continues to provide substantial benefits in the effective management of risk and security, and ensures investment in information security is commensurate with the organization's strategic direction and risk profile."

Enterprise risk management "is generally operating at a higher level of concern [than corporate security], looking at the big things that could keep the organization from achieving its mission," adds Lavagnino. "We're talking really big here—the things that would take you down as a company."

While some of the CISO/CSOs risks may rise to the enterprise level, the CRO will most likely work directly with the CIO or vice president for IT as a member of the enterprise risk management committee most of the time, and only with the CISO/CSO when more detailed information about the risk and its mitigations is needed, Lavagnino says.

"It can be hard for CISO/CSOs to accept that there are many other, more troublesome institutional risks that rank higher in likelihood and severity than their information security risks," Lavagnino says. "I also have found that the security professional is often way ahead of the game, compared to some other parts of the organization, and thus, information security risks are well mitigated."

In other words, security executives might be doing such a good job mitigating the security risks down to an acceptable level, "that they end up lower on the list of enterprise risk priorities," Lavagnino says. "That is not to say the security risks are not important; they could very well have some of the highest inherent risk ratings."

At DocuSign, all security leadership and functions report to Pageler. "However, we also have security champions embedded throughout the enterprise who have dotted line reporting into the risk team, he says. "This ensures that our line-of-business leaders and teams integrate security into their various processes, as any company's risk and security operations are only as strong and secure as its employees. Ensuring everyone is part of security helps to achieve this goal."

Helping to create a culture of security will likely be a key responsibility of CROs.

"Risk management starts at the top of these companies, and the key will be vigorous attention and collaboration between boards of directors to set stricter policies and the C-suite to communicate and implement them," King says. "This will not happen without strong executive leadership, and greater resources to manage network vulnerabilities with urgency and continual innovation."

Along with having security champions embedded throughout the organization, DocuSign prioritizes making security part of the culture through its DocuSign Emergency Response Team (DERT).

"The individuals who volunteer for DERT are trained to respond during a crisis," Pageler says. "They are trained in CPR, fire safety, and other preparedness techniques and are given awards for good security-minded acts, such as finding an open door or flagging a potential spam email." DERT members also participate in industry webinars, training and seminars to uncover and share best practices across the team.

Creating a culture of risk and security awareness for all employees in the company "is the single most important responsibility of the [enterprise risk management] and security department," Hill says. "Over the past two years we've made many enhancements to our risk and security awareness and training program in an effort to embed a vigilant security and risk awareness culture."

CRO graphic is courtesy Kevin's Security Scrapbook, April 15, 2017; Murray Associates, http://spybusters.blogspot.com/

♦♦♦

ISPLA News for INTELLENET

by

Bruce Hulme H. Hulme, CFE, BAI

ISPLA Director of Government Affairs

As this is being written, Congress has adjourned for its summer recess and is not expected to return until after Labor Day; and both major political parties are about to commence their presidential conventions. Although numerous federal regulations and measures have been offered, very little has been enacted that will affect investigative and security professionals. ISPLA and Intellenet have a memo of understanding wherein ISPLA represents Intellenet exclusively on regulatory and legislative matters. We monitor potentially adverse measures and take appropriate lobbying and political action when necessary.

This column comments on a range of issues, some of which can affect the investigative and security professional, particularly in light of recent terror attacks. I expect that several ISPLA and Intellenet board members will be attending the 2016 IASIR Conference in October. I plan to be there in my capacity with IASIR as its associate director representing state-licensed private investigators. That conference is the lead in this report. Items of varying interest follow for your summer reading.

IASIR 2016: The Nevada Private Investigators Licensing Board will host the 2016 Conference of the International Association of Security and Investigative Regulators Oct. 26-28 (Oct. 25 for the board meeting) in spectacular downtown Las Vegas.

Horrific events have shaken perceptions of security in North America and Europe. Shocking acts of terrorism, both foreign and domestic, have those in all realms of security wondering how to respond. This year's IASIR theme is "**Tuning Private Security and Investigations to the Terror Frequency: How Regulators Can Calibrate Policies to Mitigate Exposure.**" Some of the issues to be addressed are:

Is there a regulatory role in counter-terrorism? Can we increase public safety through better training? Psychological evaluations? Increased public-private collaboration in counter-surveillance efforts? Improved credentialing and enforcement?

Where do we start when we have to DO SOMETHING?

The 2016 IASIR Conference offers a significant opportunity for government and industry representatives to share ideas and develop regulatory best practices both for everyday business and the day you never want to see. Please join us in this important conversation. Details on this program and the experts presenting are at www.IASIR.org. ***See the IASIR ad on page 18.***

The IASIR 2016 venue will be the Golden Nugget Las Vegas, overlooking the dazzling Fremont Street Experience sound and light show. The hotel itself houses excellent dining, shopping and entertainment options, with even more to choose from right outside the door in the casual, easily walkable downtown area – 2 miles north of the hotspots on the Las Vegas Strip. A block of rooms has been set aside

ISPLA News continues on page 12...

for IASIR in the recently refurbished Gold Tower at the prevailing government per-diem rate of $95 per night. Rooms will be available at this rate three days prior to the conference; however, the room rate for Friday and Saturday will be $139 per night, *based on availability*. To make reservations, call the Golden Nugget at

800/331-5731 and identify yourself as an IASIR conference participant (code GSIASIR). **To receive the special rate, reservations must be made by Friday, Sept. 23.** Airline Shuttle service is available from McCarran International Airport directly to the Golden Nugget at a cost of $18 roundtrip, which includes tax and gratuity. Make reservations online at https://webbookgen.ddsefleet.com/frias/ or link from the hotel website. For more information, contact the IASIR office, 888/354-2747 or contact@iasir.org.

Fourth Amendment Issue: Warrant for StingRays

Federal District Judge William Pauley of the U.S. District Court for the Southern District of New York just ruled that law enforcement officers need a warrant before using a device that mimics cellphone towers to help track a person's mobile phone. The ongoing case is U.S.A. v. Raymond Lambis [15cr734]. The ruling was the first of its kind in federal court. It is unclear how important the precedent will be since the government has already changed its policy to require warrants going forward.

The judge excluded drug evidence gathered from a person's home after the Drug Enforcement Administration (DEA) used a cell-site simulator to track and pinpoint the precise location of the suspect's mobile phone. The devices, commonly known as StingRays, Hailstorm or TriggerFish, trick mobile phones into sending their

signal to the device instead of a cell tower by mimicking the service provider's cell tower (or "cell site") and force cell towers to transmit "pings" to the simulator. Law enforcement can use the subsequent "pings" to pinpoint the nearly precise location of a mobile phone.

"Absent a search warrant, the Government may not turn a citizen's cell phone into a tracking device," the judge opined. Perhaps recognizing this, the Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator."

This new DOJ policy to require warrants came only a week after the DEA carried out its search of the home of the defendant Raymond Lambis. The government change in policy came amid sustained criticism and lobbying from lawmakers and privacy advocates after The Wall Street Journal reported in 2014 that the government was sometimes attaching the devices to airplanes and picking up troves of data.

This case dealt with a DEA investigation in which law enforcement actually obtained a warrant to get information from the target's phone — including past numbers called and cell-site location information. But to get the exact location, the DEA used the StingRay device to track the mobile phone to Lambis's apartment. Later that same day, the DEA received consent to enter the home and found drugs and drug paraphernalia.

The judge said it did not matter that the DEA obtained permission to enter the apartment as the initial use of the tracking device was illegal. The judge said law enforcement could have easily obtained a warrant to use the device but didn't.

"Here, the use of the cell-site simulator to obtain more precise information about the target phone's location was not contemplated by the original warrant application," the judge ruled. "If the Government had wished to use a cell-site simulator, it could have obtained a warrant."

Secret NSA Program Leak: Precursor to Snowden Affair

A Washington, D.C., ethics committee has recommended public censure for a former Justice Department lawyer who leaked information about the government's warrantless wiretap program. The lawyer,

Thomas M. Tamm, had agreed to the censure for revealing confidential client information, according to a report by the hearing committee of the District of Columbia Court of Appeals Board on Professional Responsibility. He could have been suspended or disbarred. The New York Times reported on the recommendation.

> *"While, of course, lawyers are prohibited from revealing client secrets, even when it seems that it is the right thing to do, that Respondent's motivation was to try to end an illegal program through the only method he believed he had available to him is substantially mitigating, notwithstanding the fact that he now realizes there were other options available to him at the time,"* the report said.

Tamm had told a reporter about the secret National Security Agency program in a 2004 pay phone call from a subway station. Eighteen months later The New York Times ran a Pulitzer Prize-winning story on the program used to wiretap overseas phone calls and emails of terrorism suspects. Tamm suspected the program bypassed the special intelligence court and concluded it was probably illegal. The Bush administration commenced the once-secret warrantless wiretapping and bulk data collection program known as Stellarwind in October 2001. It bypassed the Foreign Intelligence Surveillance Act enabling the NSA's program of wiretapping without the court-approved warrants ordinarily required for domestic spying.

In December 2005, The Times published an article by James Risen and Eric Lichtblau revealing the warrantless wiretapping component of the program. The article won a Pulitzer Prize and prompted a huge leak investigation that came to focus on Mr. Tamm, among other people.

Tamm placed the call when he was a lawyer with the Justice Department's

Office of Intelligence Policy and Review. The hearing committee cited several mitigating factors: Tamm's intent was to further government compliance with the law, he discussed the issue with a supervisor but thought it would be futile to contact the attorney general, he received no financial compensation for the disclosure, and he was careful not to disclose details about the program.

Tamm *"… has already paid a severe price for his actions,"* the hearing committee report says. *"He was under criminal investigation for years after the disclosure. This criminal investigation was both stressful and expensive. The investigation by Disciplinary Counsel—aside from the criminal investigation—has been pending since 2009. Moreover, [Tamm] now no longer works for the Department of Justice; he is an assistant public defender in Washington County, Maryland, with a much lower salary. No reasonable person looking at what [Tamm] has gone through would think that revealing a client secret in this way is a cost-free endeavor."* Tamm admitted his violating an ethics rule against revealing confidential client information was *"very serious,"* but the committee also found that substantial factors militated against a more severe punishment. Factors considered by the committee included: He had acted as a whistle-blower; he revealed only the existence of the program, and not any operational details about it; he neither sought nor received financial gain; and he has *"already paid a severe price for his actions,"* from years of being under criminal investigation.

Uber and Ergo …

Court-ordered documents undermine Uber's claim that it knew nothing of a secret investigation: Documents show a trail from Uber to Ergo, the business-intelligence firm whose investigator used a ruse to snoop on a plaintiff.

Details have emerged about a man who has sued Uber, in a July 6, 2016 Crain's New York article by Matthew Flamm. Issues on pretexting and unlicensed investigation are likely to arise from this litigation.

A supposedly rogue investigation that Uber originally claimed it knew nothing about—and which could turn out to be a costly embarrassment for the

ride-hailing giant—began with a 10-word request from the company's general counsel. *"Could we find out a little more about this plaintiff?"* Salle Yoo wrote to Uber's chief security officer, Joe Sullivan, on Dec. 16, 2015.

That email and others documenting a trail from Uber to Ergo, the New York-based global intelligence firm that would ultimately field Yoo's request, were revealed in a federal court filing. They were entered in support of a motion for relief brought by Connecticut conservationist Spencer Meyer—the mysterious plaintiff about whom Yoo inquired immediately after Meyer filed an antitrust class-action suit charging Uber Chief Executive Travis Kalanick with price fixing.

In a motion for relief, also filed, Meyer and his lawyers added details to charges they made previously in court proceedings: Ergo, at Uber's direction, set out to dig up information that could damage the plaintiff and his lawyer, Andrew Schmidt. Furthermore, they charge, the investigator, who was unlicensed, obtained information by misrepresenting himself to his interview subjects.

Emails also show that the investigator, Miguel Santos-Neves, was hardly a misguided employee, as Ergo and Uber have claimed, but instead worked closely with Ergo's managing partner, former CIA official Todd Egeland.

"All the sources believe that I am profiling Meyer for a report on leading figures in conservation," Santos-Neves wrote to Egeland after the Ergo executive suggested the investigator go back to his sources and look deeper for Meyer's motivation in bringing the suit. "I think this cover could still protect us from any suspicion in the event that I ask" a question about the lawsuit.

In the report that was eventually provided to Uber, Ergo suggests that Schmidt could be leading the suit and using Meyer. It also highlights what could be the plaintiff's biggest weakness in carrying on the suit and dealing with its "potential backlash."

"Meyer may be particularly sensitive to any actions that tarnish his professional reputation, such as either being a witting 'tool' of his friend Schmidt's, or looking to 'cash in' on the lawsuit," the report stated, according to an excerpt in the filings. "Our research indicates that Meyer's preoccupation with his environmental career and reputation are the most important things to him professionally."

Uber officials deposed by the plaintiff said they did not know how Ergo developed its information, according to transcripts in the filings. Legal experts say that might not be a good defense.

"The picture that is painted in plaintiff's papers here is worrisome, because a lawyer should always know what their investigators are doing and how they are doing it," said Michael Ramos, chief risk and compliance officer at Manhattan-based global investigative firm Nardello & Co. "If in-house counsel retained the investigators, then they arguably had a duty to supervise their work."

Meyer and his team want reimbursement of legal costs incurred while Uber fought their requests for information, and they ask that a financial penalty be imposed on the company. They also want whatever the investigator dug up barred from use by Uber in the antitrust suit.

Judge Jed Rakoff, who is overseeing the antitrust suit in federal court in New York, in June had ordered Uber to turn over the documents, ruling that the technology company could not claim protection under attorney-client privilege. The plaintiff, he wrote, had provided enough reason to "suspect the perpetration of a fraud."

According to a court filing, Uber was due to give its response to the motion July 6. An oral argument was scheduled for federal court July 14.

Threat actors ...

The FDIC's information systems is believed to have

been breached by bad actors from China. The chief information officer of the U.S. Federal Deposit Insurance Corporation (FDIC) attempted to cover up the incident, according to a report published in July by the House of Representatives Science, Space and Technology Committee.

The report revealed that a threat group presumably sponsored by the Chinese government breached FDIC systems in 2010, 2011 and 2013. The attackers managed to plant malware on 12 workstations and 10 servers belonging to the banking regulator, including computers used by the chairman, chief of staff and general counsel.

According to the report, Russ Pittman, who was the FDIC's CIO at the time, had instructed employees not to discuss or proliferate information about the attack to avoid jeopardizing the confirmation of Martin Gruenberg in the position of FDIC chairman.

U.S. officials have often pointed the finger at China for attacks on government agencies. Security firm FireEye reported last month that the volume of Chinese cyber-espionage operations has dropped over the past months. While their volume has decreased significantly, experts say such campaigns are still being conducted, but they have become more focused and calculated.

As for the FDIC, Pittman is not the only CIO accused of wrongdoings. The agency's current CIO, Lawrence Gross, has been called out for failing to notify Congress of major incidents (i.e. incidents involving more than 10,000 records).

There had been several cases in late 2015 and early 2016 where former FDIC employees copied sensitive information for tens of thousands of individuals, but the incidents were not reported to Congress in a timely manner. Gross, who took the position of CIO in November 2015, "created a toxic work environment" and "retaliated against whistleblowers," the Science, Space and Technology Committee noted in its report.

In one example provided by the committee, a former FDIC employee in Florida copied over 100,000 files on a portable storage unit before leaving the organization. The FDIC reported that the employee had copied personal information records belonging to over 10,000 individuals, but the incident actually affected more than 71,000 individuals, banks and other entities.

The agency and its CIO attempted to downplay the extent of the incident until the FDIC Office of Inspector General (OIG) conducted an investigation and prompted the organization to report the breach to Congress. Furthermore, Gross reportedly removed a CISO who disagreed with him about whether the Florida incident should have been reported to Congress. Gross' ability to serve as CIO of FDIC is now being brought into question.

"The FDIC's repeated unwillingness to be open and transparent with the committee's investigation raises serious concerns about whether the agency is still attempting to shield information from production to Congress," the report said.

"To think that the FDIC is the only agency dealing with the malicious and absent-minded employees would be foolish. Is anyone surprised that a nation-state hacking group successfully breached another target in North America? The reality is that the amount of proprietary information residing on networks is astronomical and controlling access is paramount for any organization," Lior Div, CEO of Cybereason, told *SecurityWeek*.

"Today, proprietary data is regularly accessible to employees, as well as to various third party vendors. This gives nation-state actors and groups within China, Russia, Iran and North Korea treasure troves of IP, personal data nearly at their fingertips. In the case of hacking to the FDIC, the hackers access to extremely sensitive data can also be a basis of financial crime," Div added.

FDIC chairman Martin Gruenberg and interim inspector general Fred Gibson had been expected to testify before the committee.

Philadelphia Investigative and Security Professionals Beware:

The City's Draconian Wage Theft Ordinance ...

In a July 13, 2016 *Labor & Employment Alert* by attorney Steven K. Ludwig of Fox Rothschild, LLP, provided ISPLA with the following comments on an ordinance presently in effect in Philadelphia. Colleagues based in other major cities in the U.S. should make certain that similar ordinances are not in effect where they conduct their business.

Philadelphia now has a beefed up new ordinance that targets employers who fail to pay wages owed to employees. The law provides a cornucopia of remedies to an aggrieved employee, including:

- The creation of a wage theft coordinator position in city government. This "judge, jury and executioner" investigates allegations of "wage theft" and has the authority to impose substantial fines; deny, suspend or revoke any license issued or pending by the city for one year; and initiate suit against an employer.
- Purportedly creates a private right of action enabling employees to file suit against an employer.
- Mandates new notice and posting requirements.

What Employers Need To Know ...

Who can bring a claim under the Wage Theft Ordinance?

Employees, labor organizations or "[a] party acting on behalf of an employee to whom any type of wages is payable." So, virtually everybody.

Who is an employer?

City of Philadelphia, PA

(Bill No. 150741) AN ORDINANCE

Amending Title 9 of The Philadelphia Code, entitled "Regulation of Businesses, Trades and Professions," by creating a wage theft coordinator for the City and adding definitions, duties, penalties, fees, procedural requirements, a private right of action and other related items regarding wage theft ; all under certain terms and conditions.

THE COUNCIL OF THE CITY OF PHILADELPHIA HEREBY ORDAINS:

SECTION 1. Title 9 of The Philadelphia Code is hereby amended to add a new Chapter

as follows:

TITLE 9. REGULATION OF BUSINESSES, TRADES AND PROFESSIONS.

CHAPTER 9-4300. WAGE THEFT COMPLAINTS.

Every person, firm, partnership, association, corporation, receiver, business trust or any person or group employing any employee. So, almost everybody who pays wages. There is joint and several liability and the specter of individual liability even if the employee is employed by a corporation.

What type of claim can be asserted?

A claim for wages but only within the range from $100 to $10,000. No more, no less. The claim also must be for work performed in Philadelphia or where the employment contract underlying the claim was made in Philadelphia. Ripe for mischief because, if the employer is based in Philadelphia, the claim can easily be that the employment contract was "made in Philadelphia."

What can the city do against an employer?

The wage theft coordinator can order that wages owed be paid and impose substantial penalties. The financial penalties are up to $2,300 per violation – each week in which wages are unpaid is a separate violation. If unpaid, the city can sue to secure a judgment and will publish the identities of employers who have failed to pay and the amount of unpaid wages. The city also can seek imprisonment of the employer.

The city can "pile on" by also denying, suspending or revoking any license or permit issued by the city for one year if the employer violated "or attempted to" violate the Wage Theft Ordinance, the Pennsylvania Wage Payment and Collection Law or the Pennsylvania Minimum Wage Act. So, if the city decides that an employee was not properly paid $101.32, it can theoretically shut down an employer which employs thousands of employees for a year.

How does this impact the issuance of City of Philadelphia licenses and permits related to business enterprises?

Applicants will now be required to certify that the applicant has not been found guilty, liable or responsible in any judicial or administrative proceeding of committing or attempting to commit a violation of the Wage Theft Ordinance, the Pennsylvania Wage Payment and Collection Law or the Pennsylvania Minimum Wage Act within the past three years.

What notice must be provided to employees?

Employers must either post a poster of rights in a conspicuous and accessible place in each establishment where employees are employed or provide individualized notice to each employee. In addition, if "at least 5% of the employer's workforce" speaks a language other than English as their "first language," then notice must be provided "in the first language."

Notice about the ordinance also must be included in the employee handbook if an employer has one.

Willful violation of the posting and notice requirements is subject to a civil fine not to exceed $100 "for each separate offense."

Can an employer take action against an employee who filed a claim?

Retaliation and discrimination against a complainant are prohibited and can result in additional penalties.

Can an employee sue for unpaid wages?

The law claims to provide a private right of action to seek unpaid wages due, costs, counsel fees and penalties. How the city has the lawful authority to create a private right of action is a mystery. Employees already have the right to sue under the Pennsylvania Wage Payment and Collection Law or the Pennsylvania Minimum Wage Act so why the city thought this element to be necessary also is a mystery.

Will employees be able to use this ordinance to try and hold employers hostage if there is a dispute over wages owed?

The stakes are much higher now, so, yes. No word on how this ordinance will foster business development in the City of Brotherly and Sisterly Love.

What should an employer do now?

Amend employee handbooks to include the required information about the Wage Theft Ordinance and post notice of the ordinance in English or distribute notice to all employees. If 5% or more of the workforce has a first language other than English, provide notice in that language.

Even though parts of the ordinance probably are unconstitutional and other parts violate state law, better to avoid the quagmire of fighting the proverbial City Hall by paying all wages when due.

If you have any questions regarding this alert, please contact Steven K. Ludwig at 215.299.2164 or sludwig@foxrothschild.com or a member of Fox Rothschild's Labor and Employment Department.

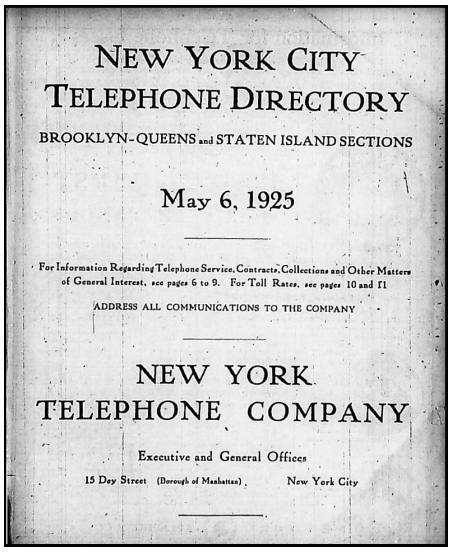
Verizon Relegates Printed Business Telephone Directories To The Shredder:

The New York State Public Service Commission has granted Verizon and its business directory publisher, Dex Media, Inc., permission to stop printing and delivering business phone books.

"Aside from not harming consumers' ability to receive directory information, we now can avoid the unnecessary printing of paper directories," said Commission Chair Audrey Zibelman in a statement. She also stated the decision is an environment-friendly one.

In 2010, New York allowed Verizon to halt the printing of phone books containing residential listings. That decision reduced about 13,600 tons of paper per year from the waste stream.

"As the vast majority of people seek this information online anyway, it's the natural progression in the digital



NEW YORK CITY
TELEPHONE DIRECTORY
BROOKLYN-QUEENS and STATEN ISLAND SECTIONS
May 6, 1925
For Information Regarding Telephone Service, Contracts, Collections and Other Matters of General Interest, see pages 6 to 9. For Toll Rates, see pages 10 and 11
ADDRESS ALL COMMUNICATIONS TO THE COMPANY
NEW YORK
TELEPHONE COMPANY
Executive and General Offices
15 Dey Street (Borough of Manhattan) New York City

age," said a Verizon spokesman. *"It doesn't make sense to continue that practice."*

Verizon is the largest telephone company in New York. In 2015 it delivered 6.3 million business directories in the state. Now it will only deliver printed directories to customers by request. It will make residential, business and government white-page directory listings available online for free for its customers.

The New York decision applies only to Verizon. Thirty-eight other local telephone companies in New York, including Taconic and Frontier, will continue to provide customers printed directories, unless they petition for a change. ♦♦♦

Bruce Hulme, CFE, BAI is ISPLA's Director of Government Affairs. More at ISPLA.org.