



# INTELNET *News*

Official Newsletter of the  
International Intelligence Network, Ltd.

*Intellenetwork.org*

*Winter 2017*



## *In this issue...*

### **PETER'S POSTING**

*By Peter Psarouthakis*.....2

**INTELNET 34TH ANNUAL CONFERENCE** .....3

**MEMBER NEWS**..... 4

**TRAVELERS WORLD THREAT MAP** .....5

**INTELNET STORIES** ..... 6

**MISSING PERSONS; FOUND FRIEND** *by Tim Young*

**ETHICAL...CAPABLE...PROFESSIONAL** *by Kitty Hailey*

### **ARE YOU A CRA?**

*By W. Barry Dixon*.....7

### **FORENSIC DOCUMENT EXAMINATIONS, PART I OF II**

*By James A. Green* .....10

**ISPLA NEWS** *by Bruce Hulme*.....12

**ISPLA UPDATE** *by Bruce Hulme*.....20

Copyright 2017, International Intelligence Network. All rights reserved. Articles are on the authority of the author. Nothing herein should be construed as legal advice. For information on our newsletter, visit the [Intellenet](http://Intellenet) web site.

# Peter's Posting

by

**Peter Psarouthakis**  
**Executive Director, Intellenet**



***Dear Intellenet Members:***

***It is now the beginning of 2017 and we are off and running ...***

**In** January we are having the first in a series of educational trainings around the United States. This is part of the Intellenet venture called the Intellenet Training Academy. This program was started as a way to tap into Intellenet's vast experience and provide training to non-members, security directors and anyone that could benefit from these programs. Of course the hopeful return on our investment in these programs is to recruit new members and to show potential clients what our members are capable of. To be clear, these programs are in no way taking the place of our annual conference. Members are of course welcome to attend any of the trainings, but if there is a choice to be made we would rather see you at our annual conferences. Our first training will occur in Florida and the second will be in Michigan this March. If you are interested in getting involved please contact Bill Blake at [billblake2@aol.com](mailto:billblake2@aol.com). Information about these programs can be found on the Intellenet website.

Our [annual conference in 2017](#) will be held in Denver, Colorado. Starting on April 20<sup>th</sup> and ending on the evening of April 22<sup>nd</sup> with our gala dinner and education fund auction. As always, we will be having a pre-day training on April 19<sup>th</sup>. This year our education committee chairman, George Michael Newman, has put together something very unique. With medical marijuana and recreational use being legalized on the state level in many states there are many security related issues that go with this. Attendees will have the opportunity to visit a fully functional grow facility and be provided a "seed to sale" presentation. After the



visit to the grow facility the group will then visit the leading provider of security services to the marijuana industry in Colorado. Attendees will get firsthand knowledge of security services that are needed for this type of industry. With more than half the states in the USA going to medical and/or recreational use of marijuana there is a place in the market share for investigative and security services. I encourage you to attend this one of a kind and first such program in any association in our profession.

Of course the rest of our conference will have many other topics and presentations from experts on topics such as investigations in South America, Europe and Australia, FCPA Compliance, forensics, business issues, etc. On Saturday morning our program will be surveillance oriented with presentation on drone use and alternatives to drones. We will end our conference with our traditional gala dinner. At this year's gala dinner we are bringing back the auction. The auction will benefit the educational fund we started at last year's conference. If you have an item to donate for the auction please contact Remi Kalacyan at [remi@spyvip.com](mailto:remi@spyvip.com).

Speaking of conferences, Intellenet will be continue to exhibit at conferences throughout 2017 as part of our ongoing recruitment campaign. If you are involved in a conference and feel it may be worth having Intellenet's booth there please contact me with the details.

I hope everyone has a successful 2017 and I look forward to seeing many of you in Denver this April.





**I**ntellenet is very excited to announce that the 34th Annual Intellenet Conference will be held at the DoubleTree by Hilton Hotel in Denver CO. The conference team, including conference host Ellis Armistead, is hard at work behind the scenes to create another successful and memorable event for all, so mark your calendars and save these dates: Wednesday April 19 – Saturday April 22, 2017!

Conference events will kick-off with a Prior Day Training event Wednesday morning April 19th, with Welcome Dinner at the hotel Wednesday evening. Seminar sessions will begin Thursday morning and end on Saturday. The conference will conclude with a Gala Dinner on Saturday evening.

#### Hotel

The DoubleTree has set up a specific registration website for Intellenet and reservations are now open! Click on this [hotel reservation link](#) and then click on the **Book a Room** button to make your reservation today. The special \$129/night room rate is available until March 29th or until the group block is sold-out, so make your reservations soon. Note: this special rate is in effective 3 days before and 3 days after the event.

The DoubleTree is a full-service hotel minutes from downtown. Features include:

- Business Center
- Fitness Center
- Free In-Room internet
- Heated indoor pool
- Non-smoking hotel
- HHonors Reward Category: 4
- and much more... check out their [website](#) for details.



# Member News

## Welcome New Members !

Felix DELGADO — Melbourne, FL

Lucas DELGADO — Melbourne, FL

Tom DENTON — Carbondale, IL

Greg RODRIGUEZ — Mexico City

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](mailto:intellenet@intellenetwork.org).

## Congratulations Remi ...

**R**emi Kalacyan and his team at VIP Investigations in Montreal, Quebec, Canada have won the Consumer Choice Award for Business Excellence for 2017. VIP has won this award every year since 2007. Seen here in a photo from last year's gala are, left to right: Marcel Sbrollini, Kristin Aslan, Remi Kalacyan and Suzanne Gosselin.

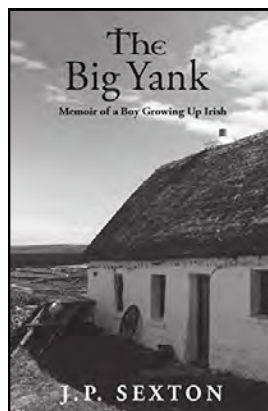


## Congratulations Jeff ...

**L**ast fall was a win for Jeff Stein and two of his clients, the accused in separate criminal defense cases. One client was cleared of homicide charges, after being jailed for 18 months in a high profile murder case in Philadelphia. The other defendant, a *pro se* client, was not prosecuted after four years in jail. Jeff presented the results of his defense investigation to the judge in chambers, with the prosecuting attorney present. The judge recommended the ADA drop all charges. Good work, Jeff.



## Congratulations John ...



**M**aybe you didn't know that from the age of nine, John Sexton was "... made to smuggle food supplies from the North of Ireland to the South, in order to increase profits from his father's restaurant business." You can learn about this and more of John's experiences on growing up in Ireland in his book, "The Big Yank," which is available in paper-

back on [Amazon](https://www.amazon.com). The book is also available on Kindle.

## Congratulations Patti ...

**P**atricia Shaughnessy was named 2016's "Investigator of the Year" by the Volunteer Lawyers Program in Arizona. Patti and her colleague Kip Johnson at Investigative Resources in Phoenix, Arizona have gone beyond the call of duty in locating biological fathers in adoption and foster care cases.

## Congratulations Rich ...

**O**ur Arizona colleagues continue to excel. Rich Robertson of Phoenix was honored with the "Freedom of Information Award" by the Arizona Newspapers Association for his hard fought success against the Pima County Attorney in a public records access battle, resulting in new case law that benefits us all.

*Continued on next page ...*

## Thank you Mayer ...

Mayer Nudell, CSC sends us his latest Traveler's World Threat Map, seen below. For more visit Mayer's web site, [www.speconsult.com](http://www.speconsult.com).

## Intellenet Members Honored ...





The committee of the 2015 Associations One Conference in Indianapolis was honored by the Society of Professional Investigators at the annual INspi Christmas

Dinner in South Bend, Indiana on December 3rd. INspi President and Intellenet member **Brandy Lord** presented the honors to Intellenet members **Bob Hopper**, Indianapolis, and **Don C. Johnson**, Bloomington, for their work in staging one of the most successful Association One conferences in recent years. Intellenet was an exhibitor and hospitality sponsor at the conference.



### Traveler's World Threat Map December 2016



-  Extreme Threat
-  High Threat
-  Medium Threat
-  Low Threat

While the information used to prepare this map is believed to be accurate, conditions since its preparation may have changed. Users should verify current conditions in the countries to which they plan travel.  
All geographic divisions are approximate.



MAYER NUDELL  
Specialized Unmanning Services

[map@speconsult.com](mailto:map@speconsult.com)

# Intellenet Stories

## MISSING PERSONS; FOUND FRIEND

*by Tim Young*

September 2016 was the 20<sup>th</sup> anniversary of a case I worked involving missing persons: Madalyn Murray O’Hair, an infamous atheist, her son Jon Garth Murray and her granddaughter Robin Murray O’Hair disappeared from Austin, Texas in 1995.

Months into the investigation, I stumbled upon another Intellenet member, Edmund Martin, also working to locate O’Hair in his capacity as an IRS Special Agent. As unlikely as it seems we ended up working together. He became a close confidant with whom I felt comfortable sharing info.

The information I obtained during my investigation did not locate the missing trio, but instead identified the three men that kidnapped and killed them. Ed Martin was the *only* law enforcement officer to take my information seriously. He was also the LEO who later pushed for and executed the apprehension of the bad guys. Ed subsequently extracted two critical confessions which led to locating the bodies of our missing trio.

Ed and I are good friends to this day.

There is much more to the story, but this is an angle that I don’t think has been covered. This is not an attempt to toot my own horn in any way, but is an example of how law enforcement (with an open mind) can work in conjunction with private investigators to obtain justice for those who can’t speak for themselves.

It is also a story about Intellenet.

*Tim Young is with Pathfinder Investigations in Sun City, Arizona, on the web at [www.timyoungprivateinvestigator.com](http://www.timyoungprivateinvestigator.com). He can be reached at [pathfinderinvestigations@cox.net](mailto:pathfinderinvestigations@cox.net).*



## “ETHICAL...CAPABLE...PROFESSIONAL”

*by Kitty Hailey*

I am proud of my accomplishments in 2016. Not overjoyed to the extent of boasting and bragging, but comfortable with my being. This profession has given me 42 years of work, income, tradecraft, education, friends and joy. It has also provided me with experiences both good and bad. I believe that with the third edition of my ethics book I have finally given back something to the life I have lived in pursuit not just of income but of quality. It’s that time of year of reflection. The seasons are shifting. It is the start of a new lunar new year and a time of self-evaluation.

I have been humbled to speak at many state and national association conferences. Somehow over time my expertise, which is extensive, has become focused solely on the area of ethics. I still work as a criminal investigator. I still perform civil rights work as a primary source of income. I spent eight years as a Capital Habeas Unit of the Federal Defenders working with the incarcerated and convicted on Death Row. I have owned and operated a large multi-service agency with dozens of employees. Yet when all is said and done the area I am asked to speak on keeps coming back to ethics. And I’m comfortable with that. This is a time in our country when the very idea of ethics is a foreign ideal. The lows that have been reached on the political stage are stunning. The depths to which people sink in degrading and maligning each other from junior high schools to the Capital steps has caused a culture of bullying, misogyny, and phobic driven hate. So being the voice of ethics makes me proud.

This year in Georgia, South Carolina, California, Massachusetts, Pennsylvania and Florida I have had the honor of addressing investigators about my topic. Orchestrating and moderating discussions on the role of ethics in the life of an investigator has been as helpful to me as to my audiences. I am excited to announce that most investigators have at least a modicum of concern for the rights of all people when conducting investigations. Some are igno-

*Continued on next page*

rant of the fact that observance of our nation's laws is vital to the continuation of our work. Being able to open up discussion about the use of drones and GPS equipment allows talk of privacy versus a need to know. Discussing the fact that locating someone can be both an exciting achievement and a potentially dangerous event has been eye-opening to many. Sharing my personal ethic of "Do No Harm" has given me a feeling of pride.

Maybe it's the season. Maybe it's the coming full moon. Whatever, I just felt the need to say to my fellow investigators around the globe, through the vehicle of Intel-  
lenet: "Thank you." You inspire me every day with the

goodness of this profession. Your good work and vital consequences elevate the conversation. I'm lucky to live in this world of ethically motivated and capable professionals. This is not reality TV. This is reality.

*Kitty Hailey is a well known investigator, conference speaker, trainer and ethicist from Philadelphia, Pennsylvania. She can be reached at [kitty@kittyhailey.com](mailto:kitty@kittyhailey.com).*



## *Are You a CRA?*

***WHAT EVERY PRIVATE INVESTIGATOR MUST KNOW ABOUT PERFORMING PRE-EMPLOYMENT BACKGROUND CHECKS THAT ARE LEGALLY COMPLIANT WITH THE FAIR CREDIT REPORTING ACT IN THE UNITED STATES ...***

*By W. Barry Nixon, SPHR, SHRM-SCP*

**P** rivate investigators and background screening firms that collect and report employment background information must adhere to the regulations of the Federal Trade Commission (FTC) under the Fair Credit Reporting Act (FCRA). The title of the legislation is potentially misleading because it infers that it deals specifically with the reporting of credit information. In fact, it also covers the reporting of information on applicants or consumers for what is determined to be a permissible purpose which includes employment inquiries. Information such as criminal records, civil records, driving records, civil lawsuits, reference checks, etc., are all considered consumer records.

It should be noted that when engaging the services of a consumer reporting agency (CRA), a.k.a. private investigator or background screening firm, both the employer and the CRA must follow the four steps outlined in the FCRA. Failure to do so can result in substantial legal exposure, including fines, compensatory damages, punitive damages and attorney fees.

It is absolute necessary that firms conducting employment background checks fully understand and comply with the FCRA.

***STEP BY STEP GUIDE TO COMPLYING WITH THE FCRA ...***

**1** A CRA may not furnish a consumer report to an employer until the employer certifies that it has given the required notice and received written authorization from the employee or applicant to obtain the report. The employer also must certify that it will comply with the DRA's requirements if it subsequently uses in

*Continued on next page*

formation from the consumer report to take adverse action with regard to the employee or applicant.

The specific FCRA requirements are explained in a document prepared by the Federal Trade Commission entitled, "Notice to Users of Consumer Report." The FCRA requires a CRA to provide a copy of that document to every employer who requests a report.

**2** Prior written disclosure/ authorization from an employee or applicant before obtaining a Consumer Report (FCRA Sections 604 and 606).

Before obtaining a consumer report from a CRA ". . . the employer must obtain written consent from the employee or applicant and provide him/her with a clear and conspicuous written disclosure that a background report may be requested." Although the disclosure must be provided in a standalone document to prevent it from being hidden in an employment application, a 1998 amendment to the FCRA clarified that the disclosure and consent may be in the same document.

It should be noted that a significant number of lawsuits have been filed over firms including other information in the written consent form beyond the disclosure and consent and/or including the consent and disclosure language in other documents such as an employment application.

CRA's typically provide these documents to an employer at no cost.

Special procedures are necessary when the employer requests a CRA to obtain employment references. If a CRA is merely verifying factual matters, such as the dates of employment or salary, no special procedure is necessary. However, if the CRA is asking for information such as job performance or personal characteristics, then this falls into a special category of consumer report called an "Investigative Consumer Report."

**Before obtaining a consumer report from a CRA "... the employer must obtain written consent from the employee or applicant and provide him/her with a clear and conspicuous written disclosure that a background report may be requested."**

When an Investigative Consumer Report is requested, there are special procedures:

- There must be a disclosure to the applicant that an investigative consumer report is being requested, along with a certain specified language. Unless it is contained in the initial disclosure, the consumer must receive this additional disclosure within three (3) days after the request is made. The disclosure must tell the applicant that they have a right to request additional information about the nature of the investigation.

- If the applicant makes a written request, then the employer has five (5) days to respond with additional information and must provide a copy of a document prepared by the Federal Trade Commission called, "A Summary of Your Rights Under the Fair Credit Reporting Act" (which the CRA should provide).

**3** Provide a copy of the Consumer Report and Notice of Rights before taking adverse action against the employee or applicant (FCRA Section 604). When an employer makes a decision to not hire an employee or

applicant this is considered an adverse action and if this decision is based on information gathered by a consumer reporting firm then the employee/applicant has certain rights.

Before taking the adverse action, the employer must provide the following information to the applicant:

- A copy of the Consumer Report
- The FTC document "A Summary of Your Rights Under the Fair Credit Reporting Act"

The purpose of these requirements is to give an applicant the opportunity to see the report that contains the information being used to make a decision about them. If the report is inaccurate or incomplete, the applicant then has the opportunity to contact the CRA to dispute or explain it. Even if there are other reasons for not hiring an appli

*Continued on next page*



cant in addition to matters contained in a consumer report, the adverse action notification procedures still apply. In a situation where tile employer would have made an adverse decision anyway, regardless of the background report, following the adverse action procedures is still the best practice for legal protection.

A common question that arises is how long an employer must wait before denying employment based upon information contained in a Consumer Report. Although the FCRA is silent on this point, the FTC staff has stated in an opinion letter that a period of five (5) business days "appears reasonable." (Brinckerhoff-Weisberg letter of June 27, 1997).

Employers are advised to consider mailing or delivery time in addition to the recommended time period to be on the safe side.

While some employers may find that the FTC's definition of "reasonable" is unworkable or unduly burdensome, caution should be exercised before taking adverse action on a more aggressive time table.

**4** Give an employee or applicant notice after taking an adverse action (FCRA Section 615)  
After sending out the documents required in Step 3, if the employer decides to take adverse action based in whole or in part on a Consumer Report, the employer must:

- Provide oral, written or electronic notice of the adverse action to the employee or applicant;
- Provide the name, address and telephone number of the CRA that furnished the report, and a statement that the CRA, "did not take the adverse action and is unable to provide the specific reasons adverse action

was taken; and

- Provide the employee or applicant an oral, written or electronic notice of his their rights under the FCRA, "to obtain a free copy of the report from the CRA and to dispute the accuracy or completeness of any information contained in the report.

All private investigators and background screening firms (consumer reporting agencies) would be wise to adhere to these four steps when conducting background checks to minimize risk and liability for their firm and their clients.

*About the Author:*



**W. Barry Nixon, SPHR, SHRM -SCP** is the COO, *PreemploymentDirectory.com*, which is the leading online directory of professional background screening firms featuring US, International and Suppliers to the background screening industry. He co-authored the landmark book, *Background Screening & Investigations: Managing Hiring Risk from the HR and Security Perspective*. He also is the publisher of award winning newsletters, *The Background Buzz* and the *Global Background Screener*. He also is the author of the *Background Checks* column in *PI Magazine*.

*In addition, Barry is an emeritus member of the elite 'Top 25 Influential People in Security' by Security Magazine.*

*You can contact Barry at 1-949-770-5264 or online at [wbnixon@preemploymentdirectory.com](mailto:wbnixon@preemploymentdirectory.com)*

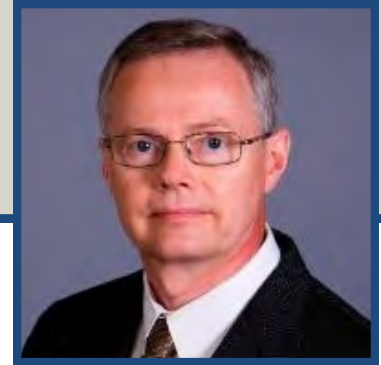
**All private investigators and background screening firms (consumer reporting agencies) would be wise to adhere to these four steps when conducting background checks to minimize risk and liability for their firm and their clients.**



# Forensic Document Examinations

## Part I of II

by  
James A. Green



### INTRODUCTION

There are numerous investigations involving documents, such as bank robbery demand notes, altered medical records, threatening or sexually harassing notes, forged contracts or wills, etc. While most of the requests received by a forensic document examiner are related to signature or handwriting comparisons, there are other examinations which may benefit your case.

### EXAMPLES OF OTHER DOCUMENT EXAMINATIONS PERFORMED INCLUDE:

**1. Recovery of indented writing.** A laboratory instrument, an Electrostatic Detection Apparatus, is used to recover the non-visible, indented writing from paper. The process does not harm or mark the document in any manner. Indentations are simply the result of writing on a page while it is placed over another page or pages. Pen pressure from the writing process disturbs the paper fibers on pages lying beneath the top page.

One example of an actual case where this instrument successfully identified the suspect involved a bank robbery demand note. The suspect had completed a job application over a notepad he used to write the note utilized in the robbery. The indented writing provided the name and address of the suspect.

**2. Ink comparisons.** An instrument called a Video Spectral Comparator (VSC), is used to examine ink in the infrared and ultra violet light spectrums. The instrument allows a non-destructive comparison of inks. A common use for the VSC is to determine if an alteration occurred on a document, i.e., medical records, contracts, wills, ledgers, etc. The alteration may be to a dollar amount, a date or other information.

Typically, when an alteration is made, the person uses the same color ink. Although pictorially the resulting alteration may appear to be the same, the ink formula, if a different pen is utilized, may be differentiated with the

VSC.

An actual case example involved an alleged alteration of a medical record which documented the death of an infant during delivery. The medical record entries recorded during the procedure, were reviewed by the plaintiff's attorney. An entry was questioned and submitted for examination. The VSC analysis determined the medication notation was originally made as a "1", and altered to a "4" by a different pen.

Prior to the document examination, the doctor had denied making the alteration during her deposition. The case was quickly settled because of the compelling evidence discovered with the VSC.

**3. Cut and paste fabrications.** Modern computer software has made signature transfers much easier, and more successful, than using the old photocopy machine process. Document examiners look for evidence of signatures or other information transferred to a fabricated document by misalignments, different fonts, different resolution, etc.

**4. Obliterations.** In many cases where a LiquidPaper® type fluid was used to cover an entry, the questioned entry may be clarified by simply holding the document to a light source. However, with thicker applications of an obliterating fluid, a document examiner may be consulted to identify the entry with special instrumentation or techniques.

Obliterations made with the use of a felt tipped pen or other writing instruments, may also be resolved through specialized instrumentation. A qualified document examiner will have the necessary instruments in their laboratory.

**5. Security features.** Passports, driver's licenses, currency and numerous other documents commonly have

*Continued on next page ...*

both visible, and invisible, security features. Special instrumentation, such as the VSC discussed previously, is used to verify specific security features of a given document.

**6. Other examinations** available include the analysis of typewritten documents, charred documents, identification of a printing process or the type of writing instrument, physical paper match comparisons, etc.

Document examiners commonly receive inquiries regarding ink dating. Although related to the field, it is not an examination document examiners conduct. Ink dating is deferred to an ink chemist. To briefly state the process, an ink chemist will extract several small ink specimens from the original document. The process will leave small holes, about the diameter of a paper clip wire, from the paper punch used. Due to the damage caused to the paper, it is considered a destructive process.

The ink is analyzed to determine the specific formula. The formula is then compared to the chemist's ink reference library to determine the manufacturer and the date it became commercially available. A practical example of ink dating is the authentication of a will. If the decedent purportedly signed a will in 2005, but the ink was not marketed until 2011, the evidence would strongly support a position the will was fabricated.

The ink dating process would be more successful with older documents because there would be a greater likelihood a pen of recent manufacture was used for the fabrication. If the document in question is from the past year or two, there are fewer pens introduced to the pen market. As a result, there is a smaller list of newer pens that could be differentiated from the document.

For recently fabricated documents, there is another ink dating process which may be of value. An ink chemist may measure the evaporation rate of the ink solvent from

the paper. The carrier (the liquid component of the ink), will evaporate at a greater rate when recently written than after the ink has aged several weeks, months or years. (The technique may be applicable for documents dated in the past two years.)

If a document was purportedly signed several months ago, but the ink from the questioned signature was determined to have a higher evaporation rate than normal for that length of time, the evidence would support a fabrication.

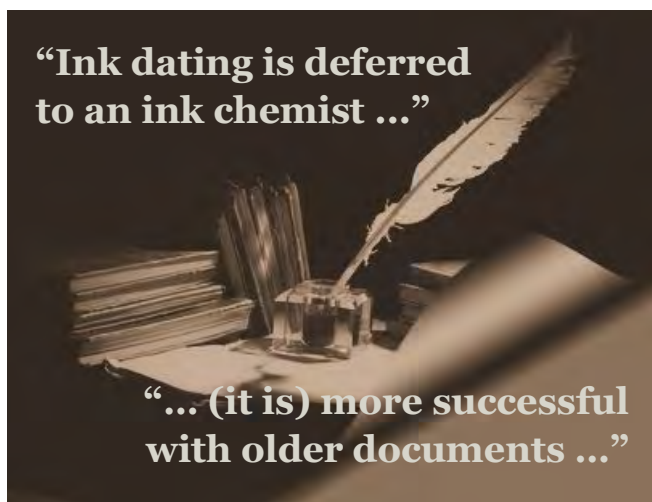
A follow-up article, Forensic Document Examinations – Part II of II, will focus on signature and handwriting comparisons.

*About the author:*

**James A. Green** is a Document Examiner and Handwriting Expert. He has a full service laboratory with a variety of modern laboratory

equipment to resolve most document examination issues and has provided testimony in the Federal and State Courts in several states. Mr. Green is certified by the American Board of Forensic Document Examiners, He also maintains active memberships in the American Society of Questioned Document Examiners, the American Academy of Forensic Sciences and the Southwest Association of Forensic Document Examiners. A 25 years veteran of the Eugene Oregon Police Department, Mr. Green can be reached at (888) 485-0832, [gdman777@aol.com](mailto:gdman777@aol.com); on the web at [www.documentexaminer.info](http://www.documentexaminer.info), on LinkedIn at <https://www.linkedin.com/in/james-green-25462b23>.

James A. Green is a member of [Intellenet's Supplemental Support List](#) of experts. This article is excerpted from Mr. Green's chapter for a new investigative "skills" book being compiled by Intellenet. For information on the book, contact Bill Blake at [billblake2@aol.com](mailto:billblake2@aol.com).





## ISPLA News for INTELNET

by

**Bruce Hulme H. Hulme, CFE, BAI**  
**ISPLA Director of Government Affairs**



### LEGISLATIVE & REGULATORY ISSUES

**T**here was no significant adverse legislation passed during the recently concluded two-year session of the 114th Congress. The fact that neither political party controlled both houses of congress contributed to the lack of any meaningful legislation being passed. However, as we now commence the 2017 first term of the two year session of the 115<sup>th</sup> Congress, one party-- the Republican-- will control the Executive branch and both the Senate and House of Representatives. In relatively short order they will most likely also achieve success in their selection of a successor nominee to the vacant U.S. Supreme Court seat previously held by the late Justice Antonin Scalia. Contrary to the belief of many of my colleagues, this situation does not necessarily portend well for our profession. I have seen in the past, that when one political party controls all branches of government legislative mischief is more likely to happen. We must do more than just monitor legislation and regulation; we must proactively lobby!

Some of the potential recurring issues in general facing our profession in the future may include the "disrupter" Trustify unlicensed practice debate, state deregulation of private investigation and security, UAS (Drones) commercial use regulation by private investigators and for physical security purposes, social media investigations, GPS tracking, anti-pretexting, anti-surreptitious surveillance, SSN redaction, public records closure legislation, and regulatory, training and vetting issues.

Over the years I have presented to Congress statements and testimony that the use of pretexts by state-licensed private in-

vestigators in conducting lawful investigations are a recognized investigative tool; that regulated investigators are an integral part of the civil and criminal administration of justice; that access to personally identifiable information is crucial to the welfare of many and often concerns not only individual physical safety but the protections of homeland security; and that that state-licensed private investigators be allowed continued access to social security numbers, dates of birth, and drivers' license numbers to assist in their important investigative mission.

It is incumbent upon our colleagues and associations such as ISPLA and INTELNET remain vigilant and ready to swiftly address Congress and regulators in a responsible and timely manner. ISPLA's bipartisan political action committee, formed in 2009, created a mechanism for individuals and professional associations to participate in lobbying and financially supporting qualified political candidates for office. Having a PAC has provided our profession with "a seat at the table rather than being the meal." Information regarding ISPLA-PAC will be the last item of this lengthy report.

### HOLOCAUST EXPROPRIATED ART RECOVERY ACT OF 2016

**A** bill of special interest to me, as the son of an artist and having investigated cases involving Nazi art ownership claims, is passage of the bipartisan effort to enact a law extending the statute of limitations to six years for the return of Nazi stolen art after identification of the stolen pieces. This bill, S2763/HR6130, the Holocaust Expropriated Art Recovery (HEAR) Act of 2016, will provide the victims of Holocaust-era persecution and their heirs a fair opportunity to recover works of art confiscated or misappropriated by the Nazis.

The measure is critical to the success of rightful owners in recovering stolen artifacts held by the Nazis. Holocaust survivors, their families, and heirs have faced over the years Kafkaesque bureaucracy and legal fights with governments, museums, gal-

leries and art collectors over ownership rights, often having their lawsuits dismissed on technicalities such as limitation statutes.

In 1998, 44 countries signed the Washington Conference Principles on Nazi Confiscated Art, urging a just and fair solution to a grievously wronged group. However, that agreement lacked the force of being law. Congressional findings estimated that the Nazis confiscated or otherwise misappropriated hundreds of thousands of works of art and other property throughout Europe as part of their genocidal campaign against the Jewish people and other persecuted groups during the WWII time period. This has been described as the greatest displacement of art in human history.

This bipartisan legislation was co-sponsored by Senators Chuck Schumer (D-NY), Richard Blumenthal (D-CT), Ted Cruz (R-TX) and John Corwyn (R-TX). The House version was sponsored by Representative Bob Goodlatte (R-6-VA). As one of the bill's sponsors stated: "Artwork lost during the Holocaust is not just property. To many victims and their families, it is a reminder of the vanished world of their families." The President is expected to sign the bill before he leaves office.

## "FREELANCE" CONTRACTORS IN THE CITY OF NEW YORK

The following emerging issue should be of interest to our investigative and security member colleagues who provide services as or for "freelance" contractors in the City of New York. Measures are presently underway to determine the feasibility of enacting similar legislation statewide. On October 27, 2016, the New York City Council unanimously passed a bill adding new requirements governing the hiring of so-called "freelancers" and imposing strong penal-

ties if a company violates the proposed law. On November 16, New York City Mayor Bill de Blasio signed into law the Freelance Isn't Free Act (Freelance Act), which formalizes the practices related to hiring freelance workers, also known as independent contractors. The Act will take effect on May 15, 2017.

The Freelance Act, will require all freelance jobs (or an aggregate of jobs over the span of 120 days) with a value of at least \$800 to be memorialized in a written contract. The contract must include the names and addresses of the freelancer and the hiring party, an itemized accounting of the work to be performed, the rate of pay and the payment date. In the event that a payment date is not specified, the bill requires payment within 30 days from the completion of the work.

The bill defines a "freelance worker" as "any natural person or any organization composed of no more than one natural person whether or not incorporated or employing a trade name that is hired or retained as an independent contractor by a hiring party to provide services in exchange for compensation." Thus, the provision is only intended to apply to those situations where a business hires an individual to complete a project rather than another business. According to this definition, a freelance worker qualifies as an independent contractor. As such, employers hiring freelancers must also ensure compliance with state and federal laws concerning independent contractors.

The bill also permits freelancers to bring claims against hiring parties who fail to pay or delay payment under contract, and prohibits hiring parties from harassing and intimidating freelancers from exercising their rights under the bill. Freelancers will be able to file complaints within two years of an alleged violation with the newly created Office of Labor Standards

(OLS), which operates within the Division of Consumer Affairs, an agency that, as we have seen, has been aggressively enforcing the New York City Earned Sick Time Act in recent years. Alternatively, a freelancer can bring a claim in civil court within six years of an alleged breach of contract and for retaliation under the bill.

A prevailing freelancer in a claim for a violation of the written contract requirement will be awarded \$250 in statutory damages and double damages for the underlying value of the contract. The bill also gives the OLS the right to bring legal action against a repeat offender and impose a penalty of up to \$25,000.

ISPLA is grateful to Fox Rothschild, LLP for providing us with this labor law alert. We will be assisting ALDONYS legislative counsel Fred Altman in assessing the likelihood of passage of similar legislation statewide in New York and to seek sponsors. Now if we can only impress the legal profession (and some private investigators who subcontract cases) to reimburse payment in a timely fashion....

## N.Y. COURT OF APPEALS' GUIDANCE FOR CLASSIFYING INDEPENDENT CONTRACTORS

An important issue for professional investigators and contract security firms about which one should be knowledgeable concerns the classification of independent contractors. On October 26, New York's highest court held that a yoga studio had properly classified its non-staff yoga instructors as independent contractors, reversing the intermediate appellate court decision that had found the contractors to be employees eligible for unemployment insurance benefits. In *Yoga Vida NYC Inc.*, 28 N.Y.3d 1013 (2016), the Court of Appeals provided guidance as to the factors that will support an appropriate independent contractor classification.

The information below furnished to ISPLA was written by the law firm of Holland & Knight.

Specifically, only yoga staff instructors, not non-staff contractors, were required to attend meetings or receive training. The yoga contractors made their own schedules and could choose their method of payment (an hourly rate or a percentage basis). Unlike staff instructors, who were paid regardless of whether anyone attended a class, non-staff contractors were only paid if a certain number of students attended their classes. Further, yoga staff instructors were restricted from working for nearby competitor studios, whereas yoga independent contractors were not so restricted and, in fact, were actually free to tell their Yoga Vida students where their other classes took place. That the studio inquired into whether the contractors had licenses, published a master schedule of classes, provided the class space, obtained substitutes when needed, and charged and collected class fees from students was considered insufficient evidence that the studio had exercised control over the contractors that would undermine their independent contractor classification.

The Yoga Vida decision provides a valuable example to any employer considering supplementing its workforce with independent contractors, whether in New York state or elsewhere. In particular, the clear distinctions drawn between policies for staff employees and contractors are a roadmap for how to properly classify workers.

There is potential tension between New York City's law and judicial standard. Employers and entities that engage independent contractors should be aware of certain tensions between the Freelance Act, which is focused

on securing payment for independent contractor services, and Yoga Vida decision, in which the court noted approvingly that the contractors were not paid if their classes were not adequately attended. Employers should know that any agreement where a contractor may not be paid for work performed may be subject to heavy scrutiny in New York City.

## EMERGING TREND IN EMPLOYMENT LAW

**In what may very well become an emerging trend in employment law, Philadelphia will become the first city to ban employers from inquiring about the wage history of job applicants.**

The law will become effective in April 2017, 120 days after it is signed by Mayor Jim Kenney.

According to a labor law alert provided to ISPLA from Fox Rothschild, LLP, the Philadelphia Fair Practices Ordinance is being amended to make it an unlawful employment practice for an employer or employment agency to inquire about a prospective employee's wage history, to require disclosure of wage history or to condition employment or consideration for an interview on the disclosure of an applicant's wage history. In addition, the law prohib-

its retaliation against a prospective employee for failing to comply with any wage history inquiry or otherwise asserting her or his rights under the new law.

The law also prohibits reliance on wage history in determining the wages to be paid or offered to a prospective employee unless the applicant "knowingly and willingly disclosed his or her wage history." The only exception is where another law "specifically authorizes the disclosure or verification of wage history for employment purposes."

The law will be enforced by the Philadelphia Commission on Human Relations, which is authorized to seek substantial fines and criminal penalties. In addition, an aggrieved person can file a private suit seeking compensatory damages, punitive damages, counsel fees, court costs and other equitable relief.

## CONCEALED CARRY RECIPROCITY ACT OF 2017 (H.R. 38)

U.S. Rep. Richard Hudson (R-NC-8) started out the New Year expanding national reciprocity rights for gun owners his top priority on the first day of his third term in Congress stating:

*"Our Second Amendment right doesn't disappear when we cross state lines, and this legislation guarantees that. The Concealed Carry Reciprocity Act of 2017 is a common sense solution to a problem too many Americans face. It will provide law-abiding citizens the right to conceal carry and travel freely between states without worrying about conflicting state codes or onerous civil suits. As a member of President-elect Trump's Second Amendment Coalition, I look forward to working with my colleagues and the administration to get this legislation*



*across the finish line.”*

Rep. Hudson’s bill, which is supported by major pro-Second Amendment groups, would allow people with a state-issued concealed carry license or permit to conceal a handgun in any other state that allows concealed carry, as long as the permit holder follows the laws of that state. It also allows residents of Constitutional carry states the ability to carry in other states that recognize their own resident’s right to concealed carry.

Hudson, who is an adviser to President-elect Donald Trump via his “Second Amendment Coalition,” introduced legislation January 3 that would guarantee concealed carry permit holders rights to have a gun outside their home state, so long as the person carrying the gun abides by local laws. The bill, Hudson says, will ensure “our Second Amendment right doesn’t disappear when we cross state lines.” The bill keeps intact any prohibitions for certain people under federal law already barred from buying or carrying a gun.

The “Concealed Carry Reciprocity Act of 2017” is a similar version of a bill he first introduced in early 2015. The newer version, though, recognizes “constitutional carry” – the right granted in some states to carry concealed firearms without a permit. The bill would also allow concealed carry in national parks and on other federal lands, including the National Wildlife Refuge System. Reciprocity across state lines for concealed carry permit holders has largely been an issue left up to states. The bill already has 58 co-sponsors.

This legislation prioritizes the rights of law-abiding citizens to concealed carry and the ability to travel freely between states without worrying about conflicting state laws. Gun control groups will argue that national reciprocity will erode state authority and public safety. For example,

some states require firearms training before one can obtain a concealed carry permit while others will issue permits to a person who has never fired a gun. Other notable differences among state laws include some where domestic violence offenders or people with restraining orders cannot get a permit. Nationwide reciprocity would also present a challenge for police officers who have no national database to determine whether out-of-state concealed carry permits are valid when a visitor is in their jurisdiction.

## **FIREARMS ACCOUNTABILITY COUNSEL TASK FORCE:**

### **Gun Control Advocates to Gain Costly Legal Advice from "White Shoe" Law Firms at Bargain Rates**

**A** December 7 article in an American Bar Association item by Debra Casen states that seven well-known law firms have agreed to provide tens of millions of dollars in free legal services to gun-control groups. Several more firms are expected to join the effort in 2017. These law firms typically invoice clients at an hourly rate in excess of \$1000.

A New York Times DealBook article identified the current law firms as: Paul, Weiss, Rifkind, Wharton & Garrison; Covington & Burling; Arnold & Porter; O’Melveny & Myers; Dentons; Munger, Tolles & Olson; and Hogan Lovells. The name of the new coalition is the Firearms Accountability Counsel Task Force.

“This effort is highly unusual in its scale,” according to the article. “Although law firms often donate time to individual causes, and some firms have worked on gun control on a piecemeal basis, the number and the prominence of the firms involved in the new coalition are unheard of for modern-day Big Law.”

The firms will help the coalition file lawsuits and draft regulatory complaints. One aim will be to overturn state laws that require businesses and local governments to allow guns on their property. Another goal is to challenge congressional restrictions on the release of data about the use of firearms in crimes. A third strategy is to develop antitrust challenges to gun industry efforts said to stifle competition, such as an effort to discourage technology that allows guns to be used only by their registered owners.

Some law firm leaders emphasized in interviews with DealBook that the overarching goal is to prevent gun violence, rather than to erode gun rights.

“There is an epidemic of gun violence in this country, and the law can save innocent lives without infringing constitutional rights,” said Brad Brian, co-managing partner at Munger, Tolles & Olson.

Our colleagues should note that three of ISPLA’s current executive committee, Al Cavasin, Peter Psarouthakis, and the undersigned, provided assistance in drafting an amicus brief on the notable “gun rights” case of *DC v. Heller*. I can tell you that the legal talent assembled above will be an exceptional adversary to the views we hold on behalf of representing the interests of armed licensed private investigators and contract security officers. The same will hold true to the NRA’s proposals for reciprocity among states for CCW permit holders.

## **INTERNET OF THINGS (IoT) & SECURITY BREACHES**

**A**n emerging issue that I expect Congress and the media to expand upon in 2017, will be the Internet of Things (IoT). On November 16, 2016, the House Subcommittee on Commerce, Manufacturing, and

Trade and the Subcommittee on Communications and Technology held a hearing, “Understanding the Role of Connected Devices in Recent Cyber Attacks.” It reviewed recent connected device-based DDoS attacks, current countermeasures, and considered future efforts to combat malicious actors that might target vulnerabilities in modern digital infrastructure. What prompted this hearing was an October 21, 2016 incident wherein, consumers were unable to reach Netflix, Twitter, CNN, and a number of other well-known websites. This was because Dyn, a company that provides core Internet services for these websites, experienced a global distributed denial of service (DDoS) attack.

A DDoS attack occurs when a malicious actor hacks into devices (referred to as “bots” and collectively as a “botnet”) and uses them to flood the targeted site with so much junk traffic that the victim can no longer serve legitimate visitors. This was the largest known DDoS attack – over one terabyte per second, approximately double the size of a similar attack two weeks prior. It leveraged hundreds of thousands of connected devices worldwide, internet-connected security cameras in particular, to mount this attack on Dyn.

This incident is one example of the risks associated with the increasing number of devices connecting to the global internet. The proliferation of connected devices, or the Internet of Things (IoT), has become a hot topic of interest. It is estimated that

50 billion devices will be connected to the Internet by 2020. While this growing technology presents many benefits for consumers and businesses across a variety of applications in health care, energy, education, transportation, agriculture, and others, unsecured devices can present an increasing number of entry points



for malicious actors to enter the network and disrupt vital communications.

Traditionally, DDoS attacks are carried out by large groups of malware-infected laptops and desktops known as “botnets.” The attack traffic generated by these botnets is exacerbated through spoofing and amplification. In a typical DDoS attack, a malicious actor floods a website with illegitimate traffic, by infecting computers with malware, which then forces the infected devices to inundate a website with illegitimate traffic. Eventually, the website is disabled because it is unable to respond to all of the traffic requests.

The recent DDoS attacks were novel, in that the botnet leveraged in the attacks was not made up of laptops and desktop bots, but malware-infected IoT devices, e.g., digital video recorders, remote home monitors, and webcams. Termed the

“Mirai” botnet after the strain of malware used to infect the bots, it successfully infected several hundred thousand devices. While the difference between computers and IoT devices may seem negligible, this fact created a DDoS attack that was unique in several ways.

First, the widespread infection and leveraging of IoT devices was novel. Second, the number of devices used meant that spoofing and amplification were not necessary; the infected devices created enough traffic to carry out a successful DDoS on their own. As most DDoS mitigation strategies rely on the detection and nullification of spoofing and amplification, stakeholders throughout the Internet struggled to respond to the attack. These factors resulted in a highly effective DDoS attack.

A prior DDoS attack occurred on September 21 leveraging the Mirai botnet against KrebsOnSecurity.com, designed to knock the website offline. It was the largest recorded attack to date with over 600 gigabits of traffic per second—“orders of magnitude more traffic than is typically needed to knock most sites offline.” Mirai was able to infect hundreds of thousands of connected devices through automatic scanning of the internet. It would search for connected devices with known username and password combinations, then use these weak credentials to take control of the devices. For some devices, the manufacturers had not provided a method for consumers to change the usernames or passwords, and many consumers were unaware that their devices were vulnerable.

In early October, source code for the malware strain Mirai was released publicly. On October 21, a DDoS



## U.S., CANADA & AUSTRALIA SUCCESSFUL ENFORCEMENT AGAINST ASHLEY MADISON SCAM

attack was launched against Dyn, a “cloud-based Internet Performance Management (IPM) company that offers, among others, DNS services.” Dyn confirmed that the malicious traffic originated from Mirai-based botnets. As a result, for two extended periods of time throughout the day, traffic was disrupted to a number of consumer-facing websites. Dyn utilized a number of mitigation techniques to restore normal traffic flows including “traffic-reshaping incoming traffic, rebalancing of that traffic by manipulation of any cast policies, application of internal filtering, and deployment of scrubbing services.” Reports indicate that malicious traffic was generated from 100,000 connected devices, mostly physically located overseas, directed at Dyn’s servers.

The Commerce Department has convened an Internet Policy Task Force, comprised of the National Telecommunications and Information Administration, the Patent and Trademark Office, the National Institute of Standards and Technology, and the International Trade Administration. It initiated a multi-stakeholder effort to promote transparency in IoT security.

The Federal Trade Commission has commenced enforcement actions against IoT device marketers. It has also produced a staff report acknowledging the many benefits of IoT, as well as making recommendations about industry self-regulation on privacy and security sensitive practices. ISPLA will keep IoT issues on our watch list.

The operators of the Toronto-based AshleyMadison.com dating site have agreed to settle Federal Trade Commission and state charges that they de-



ceived consumers and failed to protect 36 million users’ account and profile information in relation to a massive July 2015 data breach of their network. The site has members from over 46 countries.

The settlement requires the defendants to implement a comprehensive data-security program, including third-party assessments. In addition, the operators will pay a total of \$1.6 million to settle FTC and state actions.

“This case represents one of the largest data breaches that the FTC has investigated to date, implicating 36 million individuals worldwide,” said FTC Chairwoman Edith Ramirez. “The global settlement requires AshleyMadison.com to implement a range of more robust data security practices that will better protect its users’ personal information from criminal hackers going forward.”

“Creating fake profiles and selling services that are not delivered is unaccepta-

ble behavior for any dating website,” said Vermont Attorney General William H. Sorrell, “I was pleased to see the FTC and the state attorneys general working together in such a productive and cooperative manner. Vermont has a long history of such cooperation, and it’s great to see that continuing.”

“In the digital age, privacy issues can impact millions of people around the world. It’s imperative that regulators work together across borders to ensure that the privacy rights of individuals are respected no matter where they live,” said Commissioner Daniel Therrien of the Office of the Privacy Commissioner of Canada.

“My office was pleased to work with the FTC and the Office of the Canadian Privacy Commissioner on this investigation through the APEC cross-border enforcement framework,” said Australian Privacy Commissioner Timothy Pilgrim. “Cross-border cooperation and enforcement is the future for privacy regulation in the global consumer age, and this cooperative approach provides an excellent model for enforcement of consumer privacy rights.”

According to the FTC complaint, until August 2014, operators of the site lured customers, including 19 million Americans, with fake profiles of women designed to convert them into paid members. Only users who pay to access the site can use all of its features, such as sending messages, chatting online in real time, and sending virtual gifts.

According to the FTC complaint, the defendants assured users their personal information such as date of birth, relationship status and sexual preferences was private and securely protected. But

the FTC alleges the security of AshleyMadison.com was lax.

According to the complaint, the defendants had no written information security policy, no reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security.

Intruders accessed the companies' networks several times between November 2014 and June 2015, but due to their lax data-security practices, the defendants did not discover the intrusions, the agency has alleged.

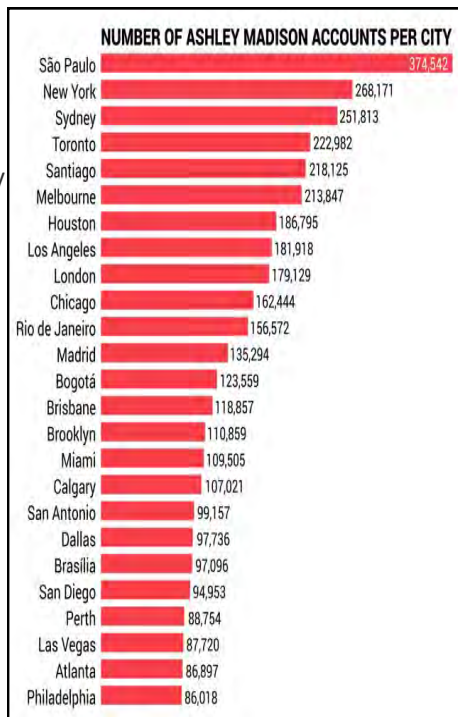
On July 12, 2015, the companies' network experienced a major data breach that received significant media coverage.

In August of 2015, the hackers published sensitive profile, account security, and billing information for more than 36 million AshleyMadison.com users. According to the complaint, this included information that the defendants had retained on users who had paid \$19 for a "Full Delete" service to purportedly remove their data from the site network.

The complaint charges the defendants misrepresented that they had taken reasonable steps to ensure AshleyMadison.com was secure, that they had received a "Trusted Security Award", and that they would delete all of the information of consumers who utilized their Full Delete service. The complaint also charges the defendants with misrepresenting that communications received by members were from actual women when in fact they were from fake engager profiles.

Finally, the FTC alleges that defendants engaged in unfair security practices by failing to take reasonable steps to prevent unauthorized access to personal

information on their network, causing substantial consumer harm.



In addition to the provisions prohibiting the alleged misrepresentations and requiring a comprehensive security program, the proposed federal court order imposes an \$8.75 million judgment which will be partially suspended upon payment of \$828,500 to the Commission. If the defendants are later found to have misrepresented their financial condition, the full amount will immediately become due. An additional \$828,500 will be paid to the 13 states and the District of Columbia.

The FTC worked with a coalition of 13 states – Alaska, Arkansas, Hawaii, Louisiana, Maryland, Mississippi, Nebraska, New York, North Dakota, Oregon, Rhode Island, Tennessee, and Vermont – and the District of Columbia to secure a settlement against the following defendants: 1) ruby Corp, formerly known as Avid Life Media Inc.; 2) ruby Life Inc., also doing business as AshleyMadison.com, and formerly known as Avid Dating Life Inc.; and 3) ADL Media Inc.

In addition, the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner provided assistance to the FTC's investigation and reached their own settlements with the company. To facilitate cooperation with its Canadian and Australian partners, the FTC relied on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

## HACKING OF PROMINENT U.S. LAW FIRMS LED TO INSIDER TRADING ARREST AND OTHER CHARGES BY U.S. ATTORNEY

The U.S. Attorney for the Southern District of New York in December announced the arrest of a Macau resident and the unsealing of charges against three individuals for insider trading, based on information hacked from prominent U.S. law firms. Iat Hong was arrested on December 25 in Hong Kong on U.S. insider trading and hacking charges. In addition to successful cyber intrusions into two law firms. The defendants were charged with attempting to hack into a total of seven law firms.

On December 27, Preet Bharara, the United States Attorney for the Southern District of New York, and William F. Sweeney Jr., the Assistant Director-in-Charge of the New York Field Office of the FBI, announced the arrest of Iat Hong and the unsealing today of a 13-count superseding indictment charging HONG, BO ZHENG, and CHIN HUNG ("Defendants"). The

Defendants are charged with devising and carrying out a scheme to enrich themselves by obtaining and trading on material, nonpublic information (“Inside Information”), exfiltrated from the networks and servers of multiple prominent U.S.-based international law firms with offices in New York, New York (the “Victim Law Firms”), which provided advisory services to companies engaged in corporate mergers and acquisitions (“M&A transactions”). The defendants targeted at least seven law firms as well as other entities in an effort to unlawfully obtain valuable confidential and proprietary information. Hong, a resident of Macau, was arrested on these charges on December 25, 2016, in Hong Kong and is now pending extradition proceedings. Hong was presented for an initial appearance on December 26, 2016, before a Judge in Hong Kong and is expected to have his next court appearance on January 16, 2017.

As alleged, from April 2014 through late 2015, the Defendants successfully obtained Inside Information from at least two of the Victim Law Firms (the “Infiltrated Law Firms”) by causing the networks and servers of these firms to be hacked. [Note: The indictment does not identify the law firm victims, but information gleaned from media coverage about the mergers indicates they are Weil, Gotshal & Manges and Cravath, Swaine & Moore.] Once the Defendants obtained access to the law firms’ networks, the Defendants targeted email accounts of law firm partners who worked on high-profile M&A transactions. After obtaining emails containing Inside Information, the Defendants purchased stock in the target companies of

certain transactions, which were expected to, and typically did, increase in value once the transactions were announced. The Defendants purchased shares of at least five publicly-traded companies before public announcements that those companies would be acquired, and sold them after the acquisitions were publicly announced, resulting in profits of over \$4 million. In each case, one of the two Infiltrated Law Firms represented either the target or a contemplated or actual acquirer in the transaction.

Companies identified in potential mergers and acquisitions through the hacking scheme included: Intermune, a publicly traded U.S.-based drug maker; Intel Corporation, a publicly traded multinational technology company, in connection with a contemplated acquisition of Altera Corporation, a publicly traded integrated circuit manufacturer; Pitney Bowes Inc., a publicly traded international business services company, in connection with a contemplated acquisition of Borderfree, Inc., a New York publicly traded e-commerce company; and were also involved in a start-up robotics company (the “Robotics Company”), started by the defendant ZHENG, which was engaged in the business of developing robot controller chips and providing control system solutions. HONG and HUNG were also involved in running the Robotics Company.

In addition to their efforts to hack the Victim Law Firms’ networks and servers during this period, the Defendants also caused confidential information to be exfiltrated from the networks and servers of two robotics companies (the “Robotics Company Victims”) using substantially similar means and methods of exfiltration as were used to access and attempt to access and ex-filtrate information from the Victim Law Firms.



**I**n October at the annual meeting of the International Association of Security and Investigative Regulators (IASIR), I was re-elected to my sixth two-year term as their Private Investigation profession representative board member. IASIR is an association of government regulators of the private investigation, contract security, alarm, and armored car industries in the United States, Canada, France, and United Arab Emirates. ISPLA's continuing role at IASIR has served our profession and INTELLENET's members well in addressing legislative and regulatory issues affecting our profession.

As Government Affairs Director for ISPLA and Legislative Liaison Board member of INTELLENET, the IASIR board position has afforded me the opportunity to work closely with the Armored Car Association, Electronic Security Association, National Association of Security Companies, and state professional association representatives.

**ISPLA-PAC: INVESTIGATIVE AND SECURITY PROFESSIONALS FOR LEGISLATIVE ACTION POLITICAL ACTION COMMITTEE**

ISPLA administers a voluntary non-partisan political action committee committed to improving and protecting the private investigative and security professions in the United States. Banding

*Continued on next page ...*

together as an industry, we make a united effort to obtain better government through education and political action.

### THE PURPOSES OF ISPLA-PAC ARE:

- 1) To promote and strive for the improvement of government by encouraging and stimulating members of the industry, and others, to take a more active and effective part in state and federal governmental affairs.
- 2) To encourage members of the investigative and security community, and others, to understand the nature and actions of their government.
- 3) To assist members of the industry, and others, to organize themselves for more effective political action.
- 4) To finance political efforts supporting state and federal legislative officeholders, and candidates that benefit the public by improving and protecting our industry.

As a part of our administration of ISPLA-PAC, we receive numerous reports almost daily and decisions of the Federal Election Commission regarding election campaigns and political action committees. At its open meeting of December 1, the Commission unanimously approved 13 legislative recommendations to send to Congress for consideration. The legislative recommendations approved by the Commission are:

### WHY YOU SHOULD SUPPORT ISPLA-PAC:

There is an urgent need to establish and maintain our industry as a strong, concerned, and active political force. When you support ISPLA-PAC, you help assure your profession's involvement in the decision-making process. The quality and nature of laws, rules and regulations affecting your business and your pocketbook are determined by elected officials. Your voluntary PAC contributions, when combined with many others, can affect who is elected - who will write the laws and enforce regulations.

### WHO MAY CONTRIBUTE TO OUR PAC?

ISPLA-PAC can only receive *Individual* contributions. Corporate contributions are prohibited.

### WHAT ARE THE BENEFITS?

Investigative and Security professionals access personal information on a daily basis. Limiting access to social security numbers, outsourcing personal information, preventing caller ID spoofing--only the tip of the iceberg. It has become clear that legislation can make or break a situation. When Investigative and Security professionals contribute to ISPLA-PAC, they are

supporting candidates who have been endorsed by the PAC because of their stand on issues important to the profession. The support is given regardless of political affiliation, and instead focuses on improving our professions.



*Bruce Hulme, CFE, BAI is ISPLA's  
Director of Government Affairs.  
You can reach Bruce at  
brucehulme@yahoo.com.  
More at ISPLA.org*



## TO CONTRIBUTE TO ISPLA-PAC:

**Send your PERSONAL check made out to  
ISPLA-PAC to the following address:**

**ISPLA**  
235 N. Pine Street  
Lansing, MI 48933



*Note: Federal law requires us to use our best efforts to collect and report the name, mailing address, occupation and name of employer of individuals whose contributions exceed \$200 in a calendar year. By making a donation you are certifying that you are at least 18 years old and making this contribution with your own personal funds – not those of another person or entity – and you meet the eligibility requirements that you are not a foreign national and are not a federal contractor.*

