# INTELLENET *News*

**Official Newsletter of the International Intelligence Network, Ltd.**

*Intellenetwork.org* *Fall 2015*

## *In this Issue ...*

# Peter's Posting

*by*

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

## Dear Intellenet Members:
## Our recruitment efforts have been paying off globally, but …

I hope everyone had an enjoyable and prosperous summer. As we are now well into the fall season there is plenty of activity going on with Intellenet. Our recruitment efforts have been paying off globally. We will continue to recruit at investigation conferences in person, as that appears to be working very well. With that being said, I think it is important to point out the reality of our association. That reality is that we have a aging membership. In the next few years we will see a high rate of retirements. We need to attract those younger professional investigators who have the ten year experience threshold that we require. Recently I was on the association website and looked at the "In Memory" page, which shows our deceased members. Along with a lot of fond memories that came to mind I was also shocked to see those who have passed in just 2014 and 2015. While you are out working, attending conferences and networking please keep a look out for new members no matter where you are located in the world.

As mentioned previously in my column, we are also beginning a marketing program directed at those that hire professional investigators. Advertising the Intellenet organization will be part of this program as well as having our vendor booth at conferences that our potential clients attend. We may need members in locations where these conferences occur to help with our booth. This will be a great opportunity for those volunteering to have direct interaction with potential clients while helping your association. More to come on this soon.

*"… I think it is important to point out the reality of our association … we have an aging membership. In the next few years we will see a high rate of retirements. We need to attract those younger professional investigators who have the ten year experience threshold that we require."*

Our 2016 Toronto conference planning is well underway. George Michael Newman has once again come up with an incredible speaker line up that will be sure to please all who attend. The conference dates are June 8-11, 2016. Hotel and other information will be posted on the listserv and website very soon. I look forward to seeing many of you there!

In the meantime, you can reach me at peter@ewiassociates.com.

♦♦♦

## COMING SOON – INTELLENET 2016 – TORONTO

# Member News

## *Welcome New Members ...*

**Leon ARMSTRONG —Williamstown, NJ**
**Victor BAZAN — Austin, TX**
**Pablo COLOMBRES — Buenos Aires, Argentina**
**Bill CONNORS — Rockland, MA**
**Ed DELISE (RETURNING MEMBER) — Jupiter, FL**
**Mark FEEGEL (RETURNING MEMBER) — St. Petersburg, FL**
**Manny FLORES — Phoenix, AZ**
**Jon GIRARD — Las Vegas, NV**
**Dejan JASNIC — Slovenia**
**Rodney KLINGE — Saipan/Guam**
**Dr. Steve MARTELLO — Hempstead, NY**
**Matt MATKOWSKI — Kennewick, WA**
**Mike MCKINLEY — Reno, NV**
**Arthur MITCHELL — Newberg, OR**
**Karen O'BRIEN — Caymen Islands**
**Rich ROBERTSON — Mesa, AZ**
**Osar ROSA — Madrid, Spain**
**Dave SHELTON — Vincennes, IN**
**Ajit SINGH — India**
**Glenn THOMAS — Albuquerque, NM**

These are our new members since we last published. To update your membership listing on the web, or in our Briefcase Roster, send info to intellenet@intellenetwork.org.

## *FOR SALE: Used train rails, gold bars ...*

A number of unfortunate email users recently received a never before seen variation of the Nigerian scam, at least new to many of us. We were offered "Used Rails" and other items at a discount price. Here is the email, verbatim, with any dangerous links removed:

*08/01/2015*

*Used Rails R50-R65 Offer*

*Dear,*

*We have large quantity of Used Rails R50-R65 for sale in Ghana West Africa, Our Prices are us$220.00 per mt CIF AWSP and us$170.00 per mt FOB Ghana payment term TT, against B/L and Inspection Report. More so, we have also 156 kg X 22 karat Gold Dust/Bar and 2,200 Cts Rough Diamond and Crude Oil for sale to any interested buyer.payment term TT, against B/L and Inspection certificate. Upon your interest on these materials you can issue your company details for FCO and details of the materials. Consequently, we have POP and Inspection Certificate of Lloyd Inspection Agent Company - Ghana, which we can send to you via fax if you request for verification.*

*If you are interested in any of these offers you are advices to contact us through this email: (DELETED) address for more information's. Don't forget to include your direct telephone number/mobile lines in your reply.*

*We are waiting for your Response. Regards and God Bless*

*Morgan Thomas*

## *The Florida Association of Private Investigator's conference had a strong Intellenet presence ...*

In addition to several members in attendance, a number of Intellenet members were seminar speakers during FAPI's annual conference: **Harriet Gold, Ray Pezolt, Kelly Riddle, Karen Smith, Ed Spicer** and **Sandra Stibbards**.

**Intellenet was an exhibitor at the FAPI conference in Altamonte Springs, Florida in September, where District Attorney Robert McCulloch of St. Louis County, Missouri was a featured speaker. Mr. McCullough's talk on the Ferguson turmoil was illuminating. In this photo, Mr. McCulloch is flanked by two well known Intellenet luminaires.**

*Member News continues on next page ...*

# Identity Crisis

By Jean Gruss | Editor/Lee-Collier

A REPRINT COURTESY OF

FLORIDA'S WEEKLY NEWSPAPER FOR THE C - SUITE

Business Observer

Friday, September 18, 2015

**Until recently, it wasn't a crime to steal a business identity in Florida.**

The woman behind new legislation to make that a criminal offense, **Carrie Kerskie**, recently became director of the Identity Fraud Institute at Hodges University. She plans to apply for $250,000 in state funding for the newly formed institute.

Thieves steal business identities to fraudulently obtain loans, credit cards and even trick banks into wiring money. "We're creating a program to let businesses know the regulations and tools and tips on how they can protect themselves," says Kerskie, a private investigator and former stockbroker with a finance degree.

Kerskie helped Florida Rep. Kathleen Passidomo and Florida Sen. Garrett Richter pass a bill this year to protect businesses from identity theft. "Now it becomes a crime, and we want to track that information," she says.

One of the reasons Florida ranks high among targets of identity thieves is the state's liberal open records law. For example, the Florida Division of Corporations publishes identification numbers that could be used by thieves to fraudulently open bank accounts, Kerskie says.

Kerskie, who recently made a presentation at Hertz' headquarters in Estero, says vendors that provide services to larger firms are unwitting portals. "The No. 1 targets are small businesses that are links to bigger fish," Kerskie says.

For example, the data breach at retail giant Target occurred through a firm that maintained the stores' air-conditioning units and was connected to Target remotely, Kerskie says. "Technology has advanced so rapidly that [companies] don't understand the information flow," she says.

Employees are the weak link in many organizations. "You could be the backdoor to a data breach just by checking your Facebook page," Kerskie says.

Thieves aren't lonely hackers or disgruntled employees. "This is organized crime," Kerskie says. Criminal organizations operate sophisticated back-office operations with hundreds of employees. "That's what we're up against," says Kerskie, who plans to send out bulletins and early warnings to businesses about the latest threats.

Education is probably the best defense against business identity theft. "Nothing in digital format can be 100% protected," Kerskie says. "We were so much better off with paper."

A special thanks to Kat Hughes, executive editor at the Business Observer for permission to share this article. And congratulations to Carrie, the new director of the Identity Fraud Institute at Hodges University.

*Continued on next page ...*

# Safeguard Your Business Identity

Business identity theft has been a growing concern as thieves capture digital information to fraudulently obtain loans, credit cards and even wire cash. Carrie Kerskie, director of the Identity Fraud Institute at Hodges University, shares tips with entrepreneurs and executives.

- Make it policy that employees can't use company emails, user names and passwords for personal use, such as for social media like Facebook. Criminals use these to access secure networks.
- Thieves will impersonate your work colleagues. The innocuous message from the accounting department may be a trick that contains a malicious link or attachment. Train employees to pick up the phone and call the sender before opening attachments or hover your cursor over the sender's address (an email address will appear on the screen) to make sure it's not someone impersonating a colleague. Likewise, you can also hover your cursor — but don't click — over any link to see if it's a legitimate link.
- Use encryption software to transmit any sensitive information.
- Create a document that identifies the people in your company or outside vendors who have access to your network and data. This could help identify breaches and alert customers in case of a problem.
- Where is the cloud? If you're considering storing data on servers outside your business, ask where those servers are physically located. You may be surprised to find out they're in vulnerable locations outside the U.S.
- Electronic medical records are vulnerable, too. Much of the software that's been developed in a rush by the health care industry to comply with government mandates lacks updated security.
- Employees with mobile devices tied into your company's network must have a password to operate. For example, that can be critical for Realtors who email contracts containing sensitive personal information from their unlocked phones.
- General business liability insurance usually doesn't cover data breaches.
- Collect as little information about customers as possible; just enough to do the job. "If you don't need it, get rid of it," Kerskie counsels.

**General business liability insurance usually doesn't cover data breaches ...**

**Collect as little information about customers as possible; just enough to do the job.**

**"If you don't need it, get rid of it," Kerskie counsels.**

♦♦♦

# Professional Etiquette When Asking for Help from Others' Contacts

**By Graham Dooley and Mike Warburton**
**INTERNATIONAL INVESTIGATORY & SECURITY CONSULTANTS**

**As an international investigator, the most valuable things you have are your lists of international contacts.**

Clearly, many of these will be from organisations like the CII and Intellenet, the value of being a member of which cannot be understated. The fact that we have a network of vetted, competent and professional investigators who can be called on at any time is immensely reassuring. However, it's a mistake to think that only other investigators can help you.

The longer one is in business, the greater are the opportunities to find useful contacts in relevant walks of life, who are able to help you in areas like specialist knowledge, or gaining access to otherwise unavailable records. These contacts are particularly helpful in areas where, for example, CII representation is low or non-existent.

These people are often important and influential in their own right, and can often pass you on to someone who is able to help you if they themselves cannot do so, particularly across international borders. They are frequently very busy in their own sphere of influence, be it politics, commerce, extraction, real estate, etc.

## POINT 1: DO NOT EXPECT OTHER PEOPLE'S CONTACTS TO WORK FOR NOTHING

Contacts will sometimes do something for you gratis, say for the purpose of returning a favour or because they trust you. However, as busy and intelligent people who may command good salaries , it is often fatal to any enterprise to expect the contact to work for nothing, particularly where the work they are being asked to do has obvious commercial value.


## POINT 2: MAKE IT VERY CLEAR AT THE START WHAT YOU WANT THE CONTACT TO DO, AND WHAT THE DEADLINE IS, AND GIVE AS MUCH INFORMATION AS YOU CAN.

Contacts are usually very willing to react quickly when an enquiry is presented that appears urgent. However, their patience can wear thin when, for example, it later transpires that the task they were asked to perform is in fact just a scoping operation to see what can be achieved in the future. Similarly, failing to reveal important information relevant to the enquiry can cause annoyance and disruption, and make you, the enquirer, look unprofessional.

## POINT 3: EXPLAIN FULLY TO THE CLIENT THAT A PARTICULAR ENQUIRY MAY TAKE MORE TIME IN LOCAL CONDITIONS.

Another issue when dealing with contacts in certain parts of the world is that clients' expectations are dictated by conditions in Europe and the USA where power, water, IT, etc. normally work 24/24. There is an expectation that, say, public record-keeping is to US standards, whereas in many places that is not the case. For example, manual record keeping is still surprisingly common throughout the world.

Internal travel in certain countries can be difficult, and the remoteness of provincial cities or inhospitable terrain can inhibit enquiries from being made other than in the capital.

I always stress the possible effect of these issues when being engaged for work in relevant countries, but it's clear that clients in the UK and USA often have unrealistic expectations of how quickly these things can be achieved.

## POINT 4: CONTACTS NEED TO BE PAID AND SO DO YOU.

*Continued on next page ...*

### INSIST ON SOME PERCENTAGE BEFOREHAND, EXCEPT IN SIMPLE CASES WHERE YOU KNOW THE RESULT CAN BE OBTAINED.

There is nothing worse than having a contact put a difficult enquiry in place in demanding conditions, and the client then loses interest and pulls out.

For which reasons, to avoid wasting the contact's time as above and avoid appearing unprofessional, it is sensible to ask for at least part-payment up front before embarking on the enquiry, in all but the most straightforward cases. The culture has also grown up of a "no result – no fee" approach to cases. This is like taking your old car to the garage and then not paying the garage when they find after much work that a car as old as this can't be fixed.

### POINT 5: UNDERSTAND THAT LIABILITY INSURANCE CANNOT BE OBTAINED TO COVER CERTAIN COUNTRIES.

It is clearly highly desirable to have professional indemnity insurance, but it has to be understood that there are some countries in the world where such coverage isn't available. Therefore, to obdurately insist that the person who is going to do the work for you signs a lengthy agreement agreeing to such insurance before you will give them a simple achievable enquiry may bring the process of engagement to a halt and make you appear arrogant.

### POINT 6: TRY TO AVOID "BIDDING WARS"

When someone offers work, several agents bid for it, and the lowest bid is accepted, this does not guarantee the client will get the best service. Unless you absolutely can't find anyone in the right area, it is better to use your networks' members' pages to source someone local to the enquiry, rather than throwing it open to everyone for a "blind auction."

Also, when a job is referred, say, from the Caribbean to the USA to England, and then to Africa, the original reasonable bid in Africa will have got inflated twice on its way back to the Caribbean, so the bid is no longer so attractive, and the subcontracting involved becomes complicated. The client may well lose interest.

This issue, we believe, is one of the main reasons that cause members to leave the various networks because the members are losing business thereby.

It might well be better for intermediate parties to take an arrangement fee rather than try to subcontract, with the resulting price increases.

### CONCLUSION:

We hope that these thoughts are helpful in your future dealings. Please don't hesitate to come back with any comments or queries.

 *Graham Dooley and Mike Warburton are former UK detectives and now international investigation and security consultants, specializing in Africa and France. For more information go to:*

- *Amethyst Global LLP (enquiries@amethyst-global.co.uk www.amethyst-global.co.uk)*
- *Anglo French Research Ltd (enquiries@anglofrenchresearch.com www.frenchinvestigations.com)*
- *Portsea Island Security and Investigation Agents (enquiries@pi-sia.co.uk www.pi-sia.co.uk)*

♦♦♦

## *Remember …*

When you need a contact or assistance in an investigation beyond your territory you can find Graham, Mike and other Intellenet members in our **Briefcase Roster.** Intellenet published this valuable resource directory annually and on our web site in the Members Only section. *(Forgot your login? Inquire at: Intellenet @intellenetwork.org)*

# The Background Buzz

*News, views and other interesting stuff for Professional Background Screeners*

## The Magnificent Seven:

### The Coming Trends that Will Impact Background Screening

By
Barry Nixon, SPHR

**"Emerging technologies will arrive that will cause catastrophic change in the background screening industry."**

When you publish the leading newsletter for the professional background screening industry (The Background Buzz) your monthly preparation involves reading hundreds of articles and publications that deal with hiring, recruiting, talent management and acquisition. Add to this numerous newspapers from around the world, business journals, blogs of every sort you can imagine and management publications. It's the price I have to pay to stay informed about what is happening in the hiring world to keep the information we provide to our readers fresh and relevant.

Distilling this down to seven key trends at one level is farcical, but from a writing perspective 'magnificent seven' flows nicely and sounds good. Conspicuously absent from my top trends are some items that are, in my opinion, inherently obvious, so I chose not to highlight them. The first is the binge that we are currently on with class action lawsuits for FCRA violations. Three more cases that I am aware of were filed in December and it is highly likely this pattern will continue into 2015. The second issue that is becoming ubiquitous is the march to use mobile technology. The use of mobile devices has stimulated a revolution in consumer marketing and selling; and is now morphing into wearable technologies. Sometime in the not too distant future there will be breakthrough for applying this technology to the hiring process and we will see unprecedented change.

My magnificent seven trends are a mixture of good news and bad news for firms involved in conducting background checks. The good news is that a number of the trends track with the growth in the job market which will feed an increase in the demand for background screening services. The bad news is that the background screening industry is a mature industry and it is only a matter of time before emerging technologies will arrive that will cause catastrophic change in the industry. We are starting to get a glimpse into some of the potential technologies that could wreak havoc; however, if history bares any witness, it is most likely to be something that none of us saw coming.

### 1 Ban-the-Box Will Become the Norm ...

The Ban-the-Box train has left the station and will continue to roll in 2015. We may even reach a tipping point where a majority of the states have passed these laws at which time a national debate will ensue about the need for one overarching federal law to ease the hodgepodge of requirements employers will need to heed.

### 2 Pre-hire Reference Assessment Tools to Rise ...

53 million Americans now freelance according to a new study which means 34% of U.S. workers are freelancing. It's a worldwide trend that is being fueled by technologies that enable and facilitate peoples' ability to work from anywhere and to have access to tools that were historically only available to major companies. So what does this have to do with background checking. Think about it! How do you verify employment of someone that is their own boss? Reference checking with freelancers' customers will enter the picture and will further fuel the growth of online pre-hire reference assessment tools. In addition, new tools will emerge to meet the need to assess of this emerging worker category.

*Continued on next page ...*

### 3 Fast Hiring Will Drive Changes ...

Fast hiring will drive changes in the fundamental way background checks are performed. Companies are striving to connect with and hire the top candidates faster than ever before. Advances in connectivity, websites, accessibility and communication platforms have made this possible. Increasingly a measure of success will become how quickly can a company pull in talent they need. According to recent article in Human Capital magazine "What many employers are currently doing is looking at traditional ways of getting resources, but realizing that these channels aren't fast enough. It takes 42 days on average to hire someone, even for short term role, and the vast majority are consequently looking to online options, which can cut this down to as little as three days."[1]

Wow! Three days!

How are you going to revamp your background checking process so it is not an impediment to fast hiring in the future? The firms that figure this one out will reap tremendous benefits and run away profits.

### 4 High Turnover Trends will Feed the Increase ...

The growth in background screening will be feed by high turnover trends. Every HR publication you read today has content focused on the high growth in turnover and the need for employee engagement to try to stem the tide of employees leaving. Unfortunately, this trend is going to escalate as the economy continues to improve and more jobs become available. Many of the people that hunkered down and stayed put during the recession are now going to make the leap.

This forebodes well for background screening firms because as the job churn continues it will increase the level background checks performed. Cha-ching!

### 5 International Screening Will Continue to Grow ...

In the international arena background screening is going to take off in China. Right now, they are in "the wild, wild west" scenario, but as more companies enter this burgeoning marketplace things are going to get really interesting. We have already seen the first lawsuit filed by a rejected applicant about improper use of background checks and also a case of the owners of a firm being sentence to prison terms for violating privacy laws. The need for standards and regulations will become very apparent and we are likely to see new laws passed relating to the background screening process as this area heats up and government exerts its control.


**"Predictive patterns in talent acquisition may put significant strain on the need for a background check."**

Fueled by several horrific incidents background checks are now required for people working in schools in India. This will increasingly move the process towards the mainstream and more industries will start to do background checks in India. This will stimulate unprecedented growth in the background screening industry.

We are on the cusp of when the number of background screening firms outside of the U.S. will rival the number of firms in the marketplace historically dominated by U.S. companies.

### 6 Big Data Will Change Everything ...

"Just like cloud computing, data protection and privacy have been all the rage and the sexy topics over the last several years—we now have a new beauty queen called "Big Data" and she is going to change everything."[2]

While it is not likely to come to fruition in 2015 the road to change is going to start to get paved as an increasing focus on talent and hiring technologies are going to emerge with the current hiring frenzy intensifying. Experts agree that big data, alongside the right data mining technology, can provide unprecedented new insights and predictive patterns into employees (not just customers), leading to improved recruitment and talent acquisition decisions which may put significant strain on the need for a background check. If employers are able to crack the

*Continued on next page ...*

code to identify the exact mix of information required to hire a candidate to succeed in a specific job who needs to do a background check. Stay tuned because the revolution will not be televised.

### 7 Move Over Linkedin ...

A new contender to the crown will emerge to compete with Linkedin as the darling of B2B social media and it will be designed for job search and use as a pre-employment screening tool unlike Linkedin. The new contender will be FCRA compliant and will give traditional background screening companies a run for their money.

I hope you enjoyed my soiree into the land of predictions and welcome your feedback and comments on my look into the crystal ball.

**Endnotes:**


1. Taylor, Chloe,'Ten workplace trends to expect in 2015,' Human Capital Magazine, Jan 7, 2015, http://www.hcamag.com/hr-news/ten-workplace-trends-to-expect-in-2015-195400.aspx.
2. Kuperman, Anna 'Notes from the iappANZ President,' ANZ Dashboard Digest, December 19, 2014, https://privacyassociation.org/news/a/notes-from-the-iappanz-president-december-19-2014/



*W. Barry Nixon, SPHR, is the COO, PreemploymentDirectory.com. He is the co-author of the book, Background Screening & Investigations: Managing Hiring Risk from the HR and Security Perspective. He also publishes The Background Buzz and The Global Background Screener which keep professional background screeners around the world informed about latest news impacting the industry.*

*PreemploymentDirectory.com is also the leading online directory of professional background screening firms featuring U.S., International background screening firms and suppliers of background screening services. Barry is a past recipient of Security Magazine's prestigious recognition having been named 'One of the Top 25 Influential People in Security.'*

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



PI REPRINTED WITH PERMISSION. THIS ARTICLE FIRST APPEARED IN PI MAGAZINE.


♦♦♦

## U.S. Senate Panel Approves a Federal "Ban the Box" Initiative

Federal agencies and government contractors would be prohibited from asking about a job applicant's criminal history until after making a conditional employment offer, under "ban the box" legislation approved October 7 by the Senate Homeland Security and Government Affairs Committee. Congress is expected to act quickly to pass the measure. The bill would cover federal executive branch agencies, along with the U.S. Postal Service, the Postal Regulatory Commission and the Executive Office of the President.

However, it would not cover job applicants for positions with federal law enforcement and national security jobs and other federal positions where the Office of Personnel Management has determined that criminal history checks are necessary.

*Extracted from Bloomberg's Daily Labor Report and other sources. For more news on labor and other employment issues, see Bruce Hulme's ISPLA Report in this issue.*


# ISPLA News for INTELLENET

By Bruce Hulme, Director of Government Affairs

**ISPLA** continues its mission to: monitor federal legislation and regulation; identify critical issues and develop policy statements; implement action plans and serve as an advocate for or against specific measures and regulations affecting our profession; proactively engage with federal lawmakers and regulators to influence legislation; administer ISPLA-PAC; and serve as a resource to the profession, government and the media. Meanwhile, below are a number of topics which may be of interest to members of INTELLENET.

## BMW to Pay $1.6 Million and Offer Jobs to Settle Federal Race Discrimination Lawsuit: *Company's Criminal Background Policy Disproportionately Affected African-American Logistics Workers, Says EEOC*

The U.S. District Court for the District of South Carolina on September 8 entered a consent decree ordering BMW Manufacturing Co., LLC (BMW) to pay $1.6 million and provide job opportunities to alleged victims of race discrimination as part of the resolution of a lawsuit filed by the U.S. Equal Employment Opportunity Commission (EEOC). The lawsuit, details about which have been previously reported by ISPLA, had been filed by the EEOC on June 11, 2013. The suit alleged that BMW excluded African-American logistics workers from employment at a disproportionate rate when the company's new logistics contractor applied BMW's criminal conviction records guidelines to incumbent logistics employees.

More specifically, the complaint alleged that when BMW switched contractors handling the company's logistics in 2008 at its production facility in Spartanburg, S.C., it required the new contractor to perform a criminal background screen on all existing logistics employees who re-applied to continue working in their positions at BMW. At that time, BMW's criminal conviction records guidelines excluded from employment all persons with convictions in certain categories of crime, regardless of how long ago the employee had been convicted or whether the conviction was for a misdemeanor or felony. According to the complaint, after the criminal background checks were performed, BMW learned that approximately 100 incumbent logistics workers at the facility, including employees who had worked at there for several years, did not pass the screen. EEOC alleged that 80 percent of the incumbent workers disqualified from employment as a result of applying BMW's guidelines were black.

Following an investigation, EEOC filed suit alleging that blacks were disproportionately disqualified from employment as a result of the criminal conviction records guidelines. EEOC sought relief for 56 African-Americans who were discharged. BMW has since voluntarily changed its guidelines.

*Continued on next page...*

BMW will pay a total of $1.6 million to resolve the litigation and two pending charges related to the company's previous criminal conviction records guidelines that had been filed with EEOC. In addition to monetary relief, BMW will offer employment opportunities to the discharged workers in the suit and up to 90 African-American applicants who BMW's contractor refused to hire based on BMW's previous conviction records guidelines. BMW also will provide training on using criminal history screening in a manner consistent with Title VII. Additionally, BMW will be subject to reporting and monitoring requirements for the term of the consent decree.

According to the EEOC, after learning of convictions, BMW responded by denying access to its facilities by anyone who had been in trouble with the law in the past -- a total of 88 workers. "Claimants were denied access to the BMW facility without any individualized assessment of the nature and gravity of their criminal offenses, the ages of the convictions, or the nature of their respective positions," the complaint said. "Moreover, they were denied plant access without any assessment or consideration of the fact that many had been workings at the BMW facility for several years without incident for UTi and prior logistics service providers."

Of those denied access to the plant because they had a criminal record, 80 percent were black and 18 percent white. The EEOC characterized those numbers as "statistically significant."

"EEOC has been clear that while a company may choose to use criminal history as a screening device in employment, Title VII requires that when a criminal background screen results in the disproportionate exclusion of African-Americans from job opportunities, the employer must evaluate whether the policy is job related and consistent with a business necessity," said P. David Lopez, EEOC's General Counsel.

**"Claimants were denied access to the BMW facility without any individualized assessment of the nature and gravity of their criminal offenses, the ages of the convictions, or the nature of their respective positions," the complaint said.**

"We are pleased with BMW's agreement to resolve this disputed matter by providing both monetary relief and employment opportunities to the logistic workers who lost their jobs at the facility," said Lynette Barnes, regional attorney for the Charlotte District Office. "We commend BMW for re-evaluating its criminal conviction records guidelines that resulted in the discharge of these workers."

EEOC enforces federal laws against employment discrimination. The Commission issued its first written policy guidance regarding the use of arrest and conviction records in employment in the 1980s. The Commission has since considered this matter in 2008 and updated its guidance in 2012. This is one of the first cases involving the use of arrest and conviction records that EEOC has filed since the Commission issued the updated guidance.

## The New York Times Editorial Board: July 29, 2015

Investigators handling criminal defense matters - along with professional investigators concerned with FOIA issues - should find The New York Times item below of interest. A version of this editorial appeared in print on July 29, 2015, in the New York edition with the headline: *Stop Hiding Police Misconduct*.

A state judge in Manhattan acted in the public interest this month when she ordered the city to release a summary of substantiated misconduct findings against the police officer who used a chokehold against Eric Garner last year during an arrest that led to Mr. Garner's death.

If the city appeals, which seems likely, the court proceedings will provide an opportunity to limit the reach of a state law that has been used to hide the employment records of police officers; even some who have committed crimes. The law is the only one of its kind in the nation.

The state statute says that an officer's personnel record cannot be publicly released or cited in court without ju-

*Continued on next page...*

dicial approval. It was enacted in 1976 to prevent criminal defense lawyers from using the state's Freedom of Information Law to request personnel records for information to use against the police in trials. But the definition of "personnel record" has grown so broad that some courts and municipalities have interpreted it to shield almost any information.

Under a broad interpretation, the disclosure law might even be used to block public access to footage from the body cameras that officers are increasingly asked to wear to monitor their conduct, warned a report last year by the New York State Committee on Open Government, which advises government, the public and the news media on freedom of information and privacy matters. As things stand now, the committee noted, the law has served "to make the public employees who have often the greatest power over the lives of New York's residents the least accountable to the public."

The case decided earlier in July by the State Supreme Court judge, Justice Alice Schlesinger, involved New York City's Civilian Complaint Review Board, an independent agency with subpoena power to investigate and make recommendations to the Police Department on disciplinary matters. The case landed in court after the review board denied the request of the Legal Aid Society, which sought a summary of substantiated complaints lodged against Daniel Pantaleo, the officer who used the chokehold on Mr. Garner.

The request focused on basic information: the number of complaints against Officer Pantaleo in which misconduct had been found before Mr. Garner's death and what recommendations, if any, the board had made to the Police Department regarding those findings. The board released such summaries for a time during 2014, but ended the practice after the city law department said it violated state law.

Justice Schlesinger said the requested summaries should be released, noting that the review board is an independent, investigative agency — not part of the Police Department — and that the summaries were limited in scope and dealt only with complaints in which police misconduct was found to have occurred.

This narrow ruling applies only to the Pantaleo case. But it points once again to the distressing fact that New York's disclosure law gives the public far less access to information about police officers than workers in virtually any other public agency.

The state Legislature needs to bring New York's disclosure laws in line with the 41 states that apply the same standard to all state employee misconduct records, including police officers. In the meantime, the courts and cities should interpret state law in a way that brings transparency to the disciplinary process. (http://www.nytimes.com/2015/07/29/opinion/stop-hiding-police-misconduct-in-new-york.html?emc=edit_tnt_20150729&nlid=46958323&tntemail0=y&_r=0)

## Pilot Reports of Close Calls With Drones Soar

Pilot reports of unmanned aircraft have increased dramatically over the past year, from a total of 238 sightings in all of 2014, to more than 650 by August 9 of this year. The FAA wants to send out a clear message that operating drones around airplanes and helicopters is dangerous and illegal. Unauthorized operators may be subject to stiff fines and criminal charges, including possible jail time.

Pilots of a variety of different types of aircraft – including many large, commercial air carriers – reported spotting 16 unmanned aircraft in June of 2014, and 36 the following month. This year, 138 pilots reported seeing drones at altitudes of up to 10,000 feet during the month of June, and another 137 in July.

Meanwhile, firefighters battling wildfire blazes in the western part of the U.S. were forced to ground their operations on several occasions for safety reasons when they spotted one or more unmanned aircraft in their immediate vicinity.

The FAA will continue to work closely with industry partners through the "Know Before You Fly" campaign to educate unmanned aircraft users about where they can operate within the rules. The agency is also supporting the National Interagency Fire Center's "If You Fly, We Can't" efforts

*Continued on next page...*

to help reduce interference with fire-fighting operations.

However, the FAA also is working closely with the law enforcement community to identify and investigate unauthorized unmanned aircraft operations. The FAA has levied drones for commercial purposes unless certified by that federal agency. Exceptions or certifications have been granted to one private investigator who is also a licensed pilot. The summer ISPLA report for INTELLENET News reports on the granting of that FAA certification to the private investigator. Similar exceptions have been granted to firms in the motion picture industry, pipeline and power line inspection companies, aerial photographers, agricultural and forestry operations and others for safety inspection, provided that the operator has a continual view of the unmanned aircraft, operates the drone in daylight no higher than 400 feet and that the drone weigh no more than 55 pounds, including the payload. Law enforcement and rescue units are also seeking exceptions.

Private investigators should be aware that the FAA prohibits the use of drones for commercial purposes. Civil penalties of $10,000 for violations of the FAA ban on using model aircraft or drones for commercial purposes, and for a number of unauthorized flights in various parts of the country have been imposed on violators. There are presently dozens of open enforcement cases.

The FAA encourages the public to report unauthorized drone operations to local law enforcement and to help discourage this dangerous, illegal activity. As the drone issue continues there will be emerging privacy issues. There will also be arguments for and against the investigative profession being granted an exception for drone video surveillance.

**There will also be arguments for and against the investigative profession being granted an exception for drone video surveillance.**

Pending federal legislation includes H.R. 798, the Responsible Skies Act of 2015, H.R. 1229/S. 635, the Drone Aircraft Privacy and Transparency Act of 2015, and Safe Skies for Unmanned Aircraft Act of 2015. The Wildfire Airspace Protection Act of 2015, would make it a federal offense to launch a drone that interferes with fighting wildfires on federal land.

States are also legislating on the subject of drones. California's Governor Brown in September just vetoed three bills that sought to block drones from flying over schools or prisons, and which would have allowed emergency personnel to shoot down a drone if it came into a fire zone. The legislation carried penalties of up to $5,000 in fines and six months in jail for drone operators.

The drone measures offered by Republican Sen. Ted Gaines also had Democratic support and carried Democratic co-authors. The bills were SB 168, SB 170 and SB 271. SB 168 sought to boost fines for operators of drones that interfere with emergency operations, and protect personnel from civil liability for shooting the drones down. SB 170 would have prohibited someone from "knowingly and intentionally" flying a drone over a prison or county jail. Gaines' other bill, SB 271, would have made it an infraction to fly a drone within 350 feet over a public school campus. Exceptions in certain cases would be made for law enforcement and the news media.

Earlier this year, Gov. Brown vetoed a bill offered by Democratic Sen. Hannah-Beth Jackson. It sought to define trespassing to include the flight of a drone to within 350 feet above a person's property. Backers of the bill, SB 142, said it helped protect people's privacy, while opponents – including the California Chamber of Commerce – said the restrictions would hinder necessary research into drone safety and efficiency.

Brown said Jackson's bill was "well-intentioned" but that it "could expose the he occasional hobbyist and the FAA-approved commercial user alike to burdensome litigation. Before we go down that path," he added in his veto message, "let's look at this more

*Continued on next page...*

carefully."

Drone regulation struggles have not been limited to states. Three years ago, President Obama signed the FAA Modernization and Reform Act of 2012, which set a September 2015 deadline for providing a safe path towards integration of unmanned drones into the national airspace. The FAA followed up on this deadline in February 2015 by releasing new rules for operating small commercial drones. Shortly thereafter, the federal Department of Justice published its own guidelines on how federal law enforcement agencies may use drones.

Between this scramble for regulations, public safety and privacy concerns, domestic drones are becoming a quickly developing technology. Earlier this year, the Consumer Electronics Association estimated that as many as 400,000 drones will be sold nationwide in 2015, with revenue from drone sales to exceed $1 billion over the next five years.

## Private Investigator Behaving Badly: Robert Williamson Pleads Guilty to Charges in Bribery Case

LAFAYETTE, LA—United States Attorney Stephanie A. Finley announced that private investigator Robert Williamson pleaded guilty to charges related to his role in a pay-for-plea scheme that garnered favorable treatment for defendants charged with various state crimes.

Prior to the start of trial, Williamson, 64, of Lafayette, appeared before U.S. District Judge Elizabeth E. Foote and pleaded guilty to one count of conspiracy, one count of bribery, and one count of Social Security fraud.

According to the guilty plea, Williamson, who is not licensed to practice law, was part of a conspiracy from March 2008 to February 2012 to solicit thousands of dollars from individuals with pending criminal charges in the 15th Judicial District. Williamson promised favorable resolutions to pending felony and misdemeanor cases, the majority of which were OWI cases. Williamson paid bribes in cash and other things of value to former personnel within the District Attorney's Office for the 15th Judicial District and employees with other organizations associated with the OWI program, including Acadiana Outreach. Williamson also obtained false and fraudulent certifications from Acadiana Outreach, which certified that his clients completed court-ordered community service, when in fact the individuals had not. Williamson would obtain fraudulent driver safety training certificates showing that Williamson's clients completed court-mandated driver improvement programs when they had not. Some of those monies were for fines, penalties and other expenses. The total fraudulent amount will be determined at sentencing. During this time, Robert Williamson also received approximately $77,677.20 from the Social Security Administration that he was not entitled to receive.

"Today marks a successful conclusion of the corruption case involving this defendant and former employees of the Lafayette District Attorney's Office," said U.S. Attorney Stephanie Finley. "This is a win for the people of our community who no longer have to be concerned about drunk drivers subverting the criminal justice system. Mr. Williamson will now be held accountable for his role in this bribery scheme and for defrauding the Social Security Administration. I want to personally thank the investigators and prosecutors who worked so diligently on this case."

Williamson faces a maximum penalty of five years in prison for the conspiracy count, 10 years in prison for the bribery count, and five years in prison for the Social Security fraud count. He also faces a $250,000 fine or both with up to three years of supervised release for each count. A sentencing date of September 25, 2015 was set.

The FBI and the Social Security Administration—Office of Inspector General conducted the investigation. Assistant U.S. Attorneys John Luke Walker and Robert C. Abendroth prosecuted the case.

*Continued on next page...*

## Another PI Behaving Badly: City of New York Department of Investigation Results in Arrest of Private Investigator on Contraband Smuggling Charges as He Tried to Visit Inmate

*(Note: The news account below broke as this article was being written. In NY one must be 25 years of age to be qualified to become a licensed private investigator. Thus far we have found no verification of such licensure. His age at time of arrest was given as 25. DOI and NYS Secretary of State have been alerted to evaluate potential charge of unlicensed PI.)*

Mark G. Peters, Commissioner of the New York City Department of Investigation ("DOI"), announced the arrest of a private investigator who was attempting to enter the George R. Vierno Center ("GRVC") on Rikers Island to visit an inmate. As part of an ongoing investigation, DOI had information that this individual had contraband and arranged for a drug-sniffing dog to screen him.

The dog alerted and the individual voluntarily surrendered approximately 66 grams of K2 synthetic marijuana and approximately 24 grams of marijuana. The contraband was concealed in the individual's underwear. DOI worked with the City Department of Correction on this investigation. DOI Commissioner Peters said, "This arrest is another example of DOI's focused investigation to stop contraband trafficking in our City's jails. A canine unit alerted that there were drugs on this visitor demonstrating why DOI's recommendation to place drug-sniffing dogs at entrances is critical."

Marrion-Paul Small-Williams, 25, of Manhattan, N.Y. was charged on October 2, 2015 with Promoting Prison Contraband in the First Degree, a class D felony; two counts of Promoting Prison Contraband in the Second Degree, class A misdemeanors; and Unlawful Possession of Marijuana, a violation. Upon conviction, a class D felony is punishable by up to seven years in prison, a class A misdemeanor by up to a year's incarceration; and a violation by a fine of up to $100. The defendant is awaiting arraignment.


According to the criminal complaint, the defendant had two clear plastic bags that each contained a dried, green leafy synthetic substance with a distinct odor and two balloons that each contained a dried green leafy substance with a distinct odor. According to DOI's investigation, a roll of electrical tape was also found concealed in the defendant's underwear. Electrical tape is often used for wrapping contraband.

DOI Commissioner Peters thanked DOC Commissioner Joseph Ponte, DOC Deputy Commissioner Michael Blake, and Bronx County District Attorney Robert T. Johnson, and their staffs, for their assistance in this investigation.

A criminal complaint is an accusation. A defendant is presumed innocent until proven guilty. DOI is one of the oldest law-enforcement agencies in the country and is New York City's corruption watchdog. Investigations may involve any agency, officer, elected official or employee of the City of New York, as well as those who do business with or receive benefits from the City.

## FLSA Settlements Will Need Court Approval: Ruling May Affect INTELLENET'S Large Investigative and Security Firms, and their Clients in NY, CT & VT, according to Fox Rothschild LLP Reports

Settlement of wage and hour actions just got harder in New York, Connecticut and Vermont. On August 7, 2015, in *Cheeks v. Freeport Pancake House, Inc.*, the United States Court of Appeals for the Second Circuit, which covers New York, Connecticut, and Vermont, issued a decision that prevents parties from stipulating to the dismissal of a case in which there are claims alleging violations of the Fair Labor Standards Act ("FLSA"). Generally, when parties settle a federal court action, they simply file a stipulation that dismisses the case with prejudice. By filing such a stipulation, the parties do not have to provide the court with a copy of their settlement agreement and the terms of any such agreement can remain private and

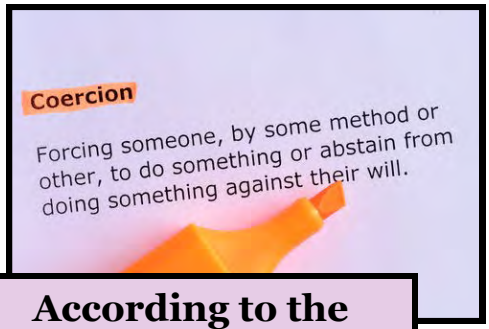
*Continued on next page...*

confidential. In *Cheeks*, the Second Circuit held that parties cannot dismiss FLSA cases by stipulation and instead the parties must submit their settlement agreement to the District Court for review so that the District Court can determine whether the settlement is fair and equitable.

*Cheeks* is a problematic decision for employers as it will make it harder to resolve FLSA claims. Because courts will scrutinize FLSA settlement agreements before they will dismiss an FLSA case, defendant-employers will find it difficult to include confidentiality and other provisions in an agreement that are normally contained in settlement agreements. Further, defendant-employers run the risk of settling an FLSA case and exposing themselves to other lawsuits. As such, employers must be vigilant in ensuring their continued compliance with the FLSA

In *Cheeks*, the plaintiff, Dorian Cheeks, had worked for the defendant, Freeport Pancake House, Inc., as a restaurant server and manager. In August 2012, she filed a complaint in the United States District Court for the Eastern District of New York alleging that Freeport Pancake House did not properly pay her overtime in violation of the FLSA and New York Labor Law. Plaintiff sought to recover overtime wages, liquidated damages, attorneys' fees, and costs. The complaint was filed as a single-plaintiff action; it was not filed as a class or collective action.

During discovery, the parties privately settled the matter. They submitted a stipulation of dismissal with prejudice to the District Court. However, the District Court rejected the stipulation holding that the parties could not agree to a private settlement of an FLSA claim absent court or U.S. Department of Labor approval. As such, the District Court directed the parties to file a copy of the settlement agreement on the public docket and explain to the court why the settlement was fair and reasonable. The parties refused and instead appealed the District Court's ruling to the Second Circuit.




**According to the Second Circuit, the FLSA has unique policy considerations and goals, namely to protect low-wage employees with unequal bargaining power who are more susceptible to coercion ...**

The Second Circuit in *Cheeks* had to address whether the FLSA permits parties to dismiss lawsuits by stipulation. The Second Circuit acknowledged that the FLSA itself was silent on the issue as were the Federal Rules of Civil Procedure. The Second Circuit also conceded that neither the Supreme Court nor any Circuit Court had ever addressed the issue. However, the Second Circuit noted that in two cases from the 1940s, the Supreme Court held that employees could not generally waive their rights. Further, the Second Circuit stated that an Eleventh Circuit decision from 1982, which has been widely followed, held that employees could only settle claims under the FLSA if there was a bona fide dispute and the settlement was overseen by a court or the Department of Labor.

The Second Circuit then reviewed the underlying policy considerations of the FLSA and the rationale used by the Supreme Court and the Eleventh Circuit in reaching their decisions. According to the Second Circuit, the FLSA has unique policy considerations and goals, namely to protect low-wage employees with unequal bargaining power who are more susceptible to coercion and more apt to accept unreasonable, discounted settlements. Thus, the Second Circuit held that the FLSA is different from all other employment statutes.

In fact, the Second Circuit noted that many District Courts had rejected FLSA settlements because of such alleged coercion and abuse. Examples that the Second Circuit cited include "a battery of highly restrictive confidentiality provisions," overly broad release provisions that would waive all possible claims against the defendants including claims that have no relationship to wage and hour issues, and attorneys' fees provisions that allow plaintiffs' attorneys to recover a substantial percentage of the recovery. Accordingly, the Second Circuit held that parties cannot dismiss FLSA cases with prejudice pursuant to stipulation.

*Continued on next page...*

Instead, they must submit their settlement agreements to the District Court for review.

After *Cheeks*, FLSA cases within the Second Circuit will be more difficult to resolve for a number of reasons. First, no matter how frivolous the allegations, parties will no longer be able to quickly resolve their differences if the plaintiff alleges a violation of the FLSA. Instead they will have to submit their settlement to a court for its approval. This would be required even if the defendant has not appeared in the action because the settlement was reached before the defendant responded to the complaint.

Second, it will be very difficult to make any FLSA settlement confidential. One of the main provisions that most defendants seek in resolving any lawsuit, including an FLSA lawsuit, is that the settlement will be confidential. Currently, when a District Court reviews a settlement agreement, the agreement is placed on the public docket. If parties are now going to be required to submit their FLSA settlements to a court for approval, in most cases, the settlement agreement will be on the public docket where anyone can review its terms. This will nullify any confidentiality provisions contained in FLSA settlements.

Third, in holding that FLSA cases cannot be dismissed by stipulation, the Second Circuit noted that there have been "abuses" in FLSA settlement agreements. Among the "abuses" noted by the Second Circuit are overly broad releases that go beyond wage and hour matters. This is a significant problem for defendants. The Second Circuit clearly disapproved of general releases contained in FLSA settlements.

Defendants now risk courts rejecting settlement agreements because they contain general releases; and if a settlement agreement contains a release limited to wage and hour matters only, defendants risk paying a settlement and having the plaintiff file a claim for non-wage and hour violations. Thus, defendants will not have security that once the settlement is finalized all issues between the parties will be resolved.

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

♦♦♦

**Intellenet members enjoy a laugh at the Associations One Conference in Indianapolis in April. Left to right: Ken Shelton, Diana Garren, Don C Johnson, Peter Psarouthakis, Brandy Lord, Jim Carino, Kevin McClain, Bob Hopper and Bill Blake.**