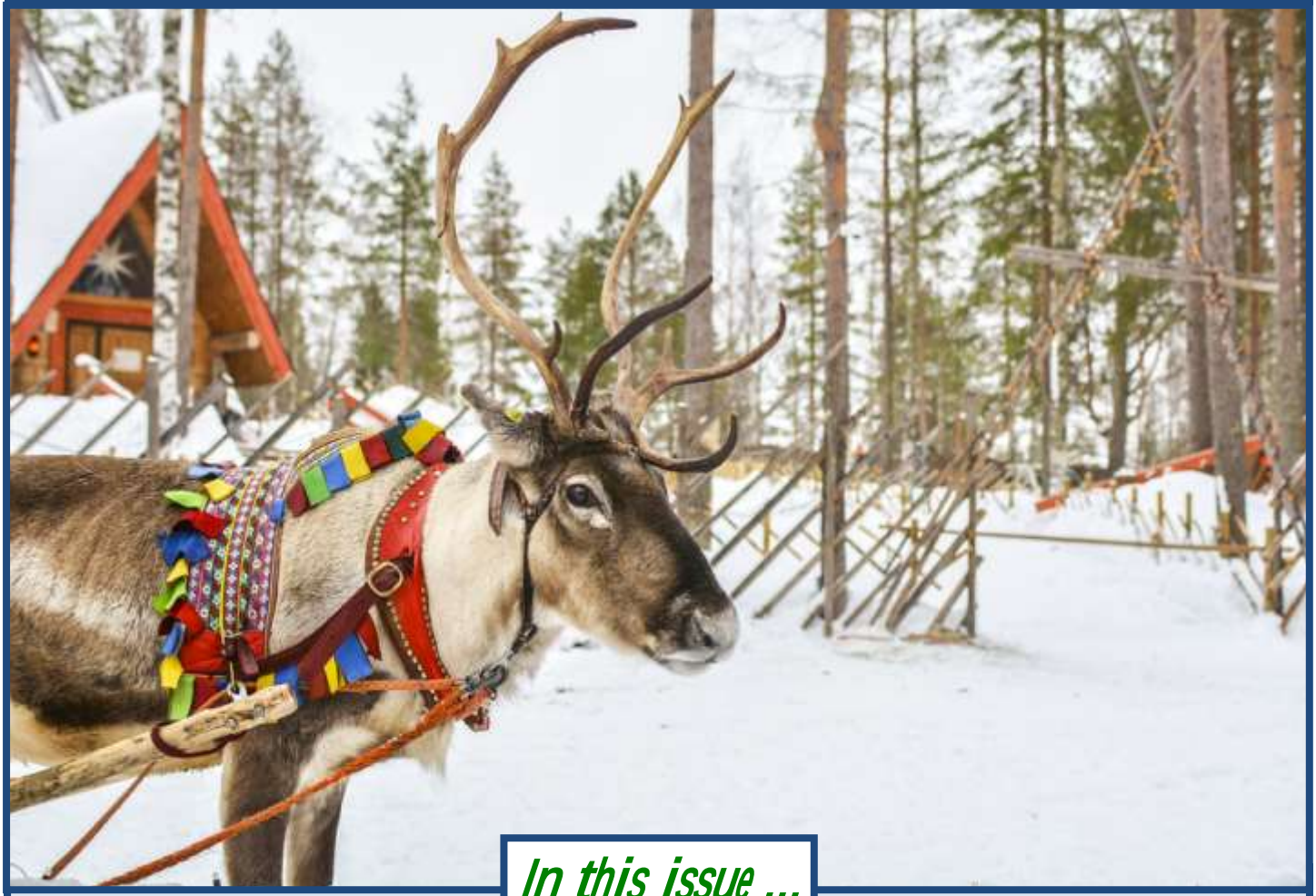
INTELLENET *News*

Official Newsletter of the International Intelligence Network, Ltd.

Intellenetwork.org *Fall 2018*



In this issue ...

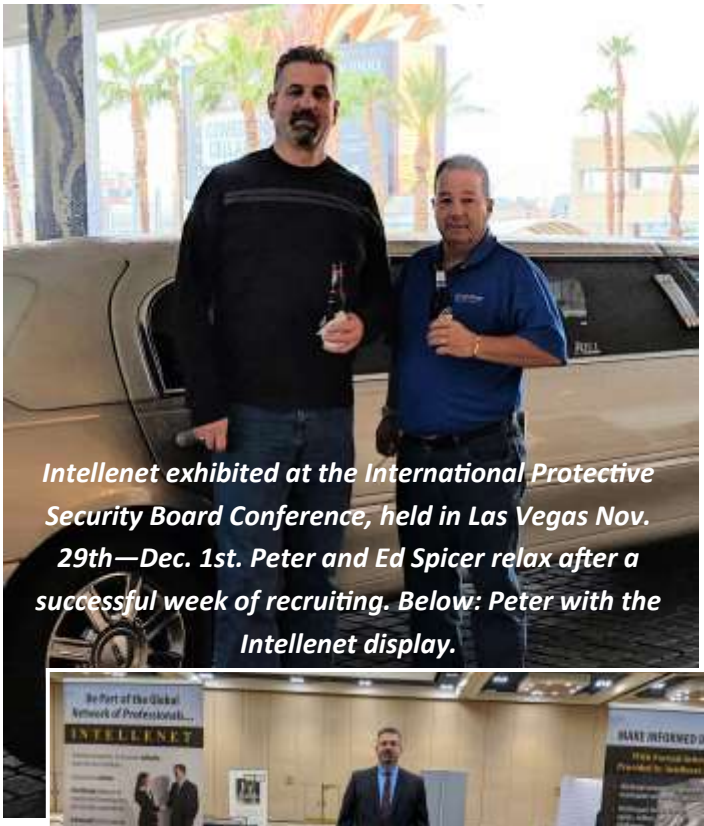
Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet

Dear Intellenet Members: Our recruiting efforts are paying off …

We are now headed into the winter months and holiday season. As I am typing this we are getting our first snow fall here in Michigan. Intellenet leadership has been very busy this year promoting the association to potential clients and recruiting new members around the globe. These efforts have paid off tremendously as we have seen many new members come into our ranks this year. I am also hearing that our efforts to promote Intellenet and its members to potential clients is paying off. More and more I have been told that clients are visiting our website or saw us at conference. A current example of these marketing efforts is our going to the International Protective Security Board conference being held in Las Vegas at the end of November. Myself and co-executive directors Ed Spicer and Jeff Stein attended this event to market Intellenet members. The number of attendees was over 300.



Intellenet exhibited at the International Protective Security Board Conference, held in Las Vegas Nov. 29th—Dec. 1st. Peter and Ed Spicer relax after a successful week of recruiting. Below: Peter with the Intellenet display.

Make no mistake about it, Intellenet is a business association for investigators and security professionals and not just a social group. Networking, helping each other and pushing clients to our members are our priorities.

We are in the process of creating a new and exciting website to help promote the association and make it more user friendly for the membership. Once the announcement that this new website is live I encourage everyone to take a few minutes to familiarize yourself with it. Some key improvements will be individual usernames and passwords to enter the "members only" section, the ability for individual bio's next to your listing, and the website will be available in many languages for those that do not read English. This new website will also play an import role in our marketing program.

The year has gone by quickly. It is certainly not too early to plan for our 2019 conference being held at the Marriott City Center Hotel located in Charlotte, NC. The dates of the conference are April 2-5, 2019. To make your hotel reservations go to http://intellenetwork.org/Annual-Conference.aspx.

Once the new website is operational we hope to have all the conference program and registration information available.

I wish everyone a great and safe holiday season and I hope to see many of you soon.

♦♦♦

Member News

Welcome New Members ...

Eduardo (Eddie) BERMUDEZ (reinstated) — Managua, NICARAGUA

Clay BILES — MEXICO

Gary COULHART — Loftus NSW, AUSTRALIA

Cary CZAPLEWSKI — Milwaukee area, WI

Frank DeANDREA — Hazelton, PA

Sandra DeANDREA — Hazelton, PA

Dennis DRISCOLL — Tewksbury, MA

Peter GALLO (reinstated) — Harrison, NY

Elaine GILL — Peabody, MA

Gamal Abdel HAFIZ — Dallas, TX

Rick HESSIG — Louisville, KY

Polycarpos (Polys) KYRIACOU — CYPRUS

Gary MARCELIN — Miramar, FL

Chris MAY — Lausanne, SWITZERLAND

Leonard (Lennie) NERBETSKI — W. Trenton, NJ

Jose NEWMAN — Chula Vista ,CA

Mike O'ROURKE — Wilmington, DE

Michael PAVONE SR — Worcester (Metro), MA

Anthony (Tony) RAYMOND — Holderness, NH

Ray RODRIGUEZ — Ft. Worth, TX

Tina SKIRVIN — Bloomington, IN

Robert (Rob) SMITH — Cape Cod, MA

Fabrice TOUATI — Sur Seine (Paris), FRANCE

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.

Great Job, Intellenet Recruiting Team!

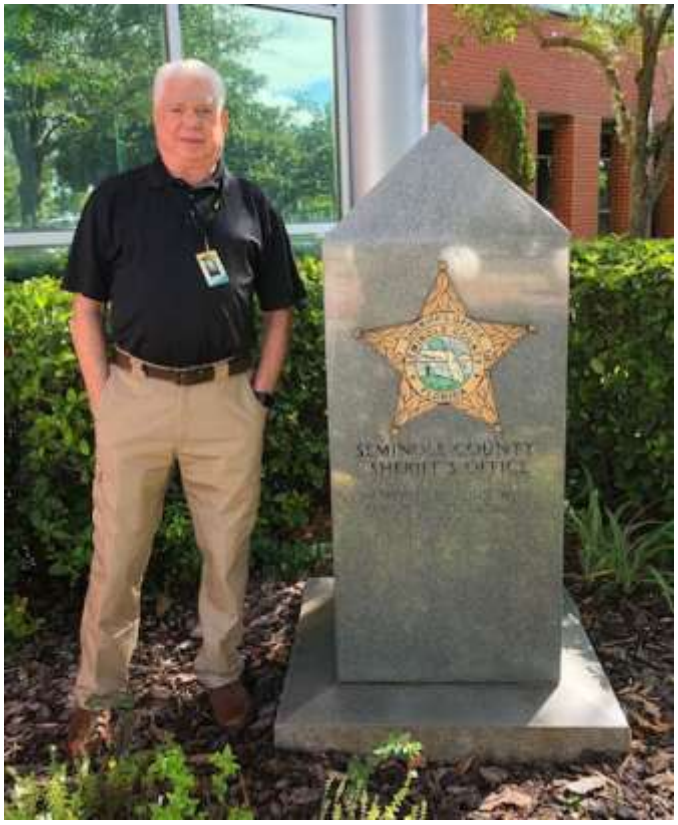
Speaking of recruiting and ...

Ed Spicer is a key recruiter for Intellenet. In addition, Ed recently posted thanks to Intellenet members who were speakers at the 1st Annual Intellenet/NEPIN Fall Seminar in New England. Pictured here: Top row, Intellenet members, left to right; **Elaine Gill, Denny Crowley, Thomas Howard**. Bottom row, left to right; members **Robert Wile** and **Dan Loper**; and Commonwealth of Mass. ABCC Senior Investigator **Carrie Guarino.**

Intellenet members take to pen ...

Intellenet members are featured prominently in the Sep-Oct issue of PI Magazine. Congratulations to **Bill Blake** for his article, "Subcontracting as a Revenue Generator"; and to **Jeff Stein** for his article, "Is There Really Truth and Justice for All?" **Jim Nanos**, PI Magazine's publisher, authored "Selecting a Surveillance Vehicle"; and regular columnist **Bruce Hulme** authors "ISPLA Insights." In the Nov-Dec issue, member **Bill Clutter** writes about a man who spent 36 years in prison for a crime he didn't commit; and featured in the PI Agency Profile article is member **Sheila Wysocki,** in an article titled: "PowerHouse PI."

MEMBER NEWS CONTINUES ON NEXT PAGE ...



A new Deputy Sheriff's in town ...

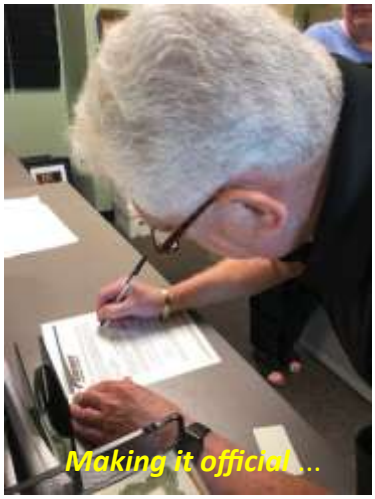
Harvey Morse, a longtime Intellenet member, has been in law enforcement over 57 years. He has served at the federal, state, county and municipal levels.

He has been a Sergeant and Advisor to the Director of the Florida Highway Patrol, an Assistant Police Chief and, until July of this year, a Sergeant with the Holly Hill Police Department, which is adjacent to Daytona Beach,

On September 13th, after completing exhaustive testing including a full medical workup, Harvey was sworn in as a Deputy Sheriff in Seminole County, Florida, where he once ran for the position of Sheriff years ago.

He graduated the Florida Police Academy at age 49, and finished 1st in his class of 82 cadets, most half his age.

Although there are no statistics available, it seems unquestionable that Harvey has become the oldest "new" Deputy Sheriff in the county's history, if not the state. Harvey turned 77 in November. Congratulations, Harvey!



Making it official ...

Congratulations to Eileen Law, the first recipient of PALI's new "Jim Carino Professional Investigator of the Year" award ...

And who better to present the award than **Jim Carino** himself, at this year's annual conference of the Pennsylvania Association of Licensed Investigators. Eileen was "shocked, humbled and honored." Here's more of what she wrote about it:

"My father always taught me to 'never judge a man until you've walked a mile in his moccasins' and I will always strive to do that. My mother taught me to 'give back' and always remember two words: She'd say 'Thank you' are two very little words, but they mean so very much."

Congratulations to TALI's new president, Ed Martin...

The Texas Association of Licensed Investigators elected **Edmond J. (Ed)Martin, CFE, TCI** as its new president at its annual conference this year. Ed is a principal and chief investigator at Sage Investigations, LLC in Austin.

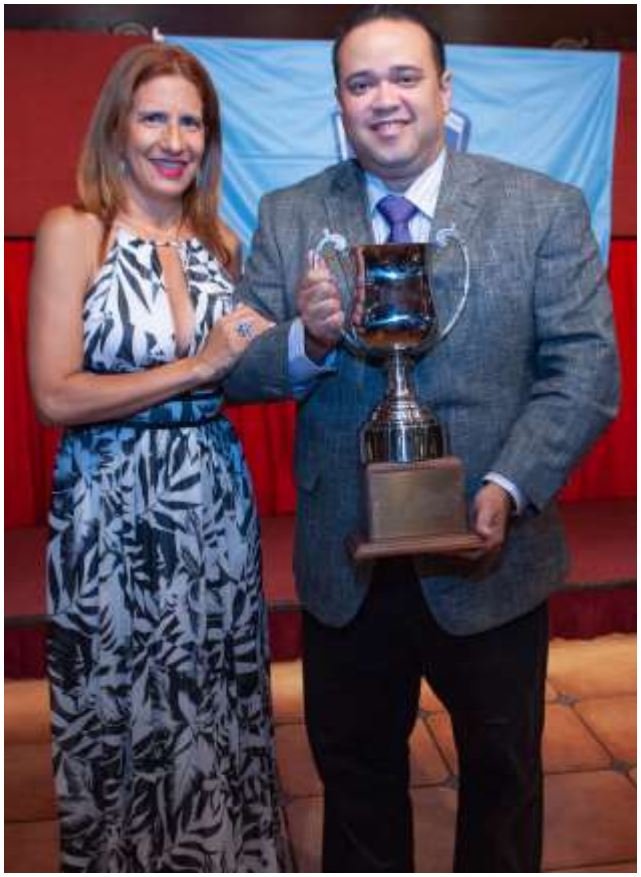
TALI has already announced its 2019 conference and seminar schedules. On February 22nd in Hurst, TALI will hold their North Texas Midwinter Seminar; the Houston Area Midwinter Seminar will be on February 8th; the 2019 Annual Conference will be held in San Antonio July 17th to the 20th at the Wyndham Riverwalk Hotel. Details on these events at TALI.org.

MEMBER NEWS CONTINUES ON NEXT PAGE ...

Bruce Hulme receives Life Award from IASIR ...

Bruce (in photo above, left) was recognized was his many years of dedication at the annual conference of the International Association of Security and Investigative Regulations in Scottsdale, Arizona in October. Bruce has been the investigative profession representative on the IASIR Board of Directors almost since its beginning, but decided not to run for the position this year. The board is compromised of licensing regulators from several states and provinces, and, most recently, South Africa. Each industry represented by the licensing authorities— investigation, security, alarm, armored car— has a non-voting member on the IASIR board, elected by their peers who are in attendance at the conference. Presenting the award to Bruce was IASIR's newly elected Vice President, Intellenet member **Don C. Johnson** (with Bruce in photo).

Fernando Fernández receives CII's Investigator of the Year Award ...



Fernando, seen here with award and wife Sophia, is founder and President of Covert Intelligence, LLC in Puerto Rico. He received the Investigator of the Year Award from the Council of International Investigators (CII) at their 2018 Annual General Meeting in Hong Kong.

Fernández received the award for his pro-bono investigative work searching for missing persons following the disaster caused by Hurricane María in his native Puerto Rico, and the subsequent development of his Viral Investigative Methodology.

After Hurricane Maria, Fernando

MEMBER NEWS CONTINUES ON NEXT PAGE ...

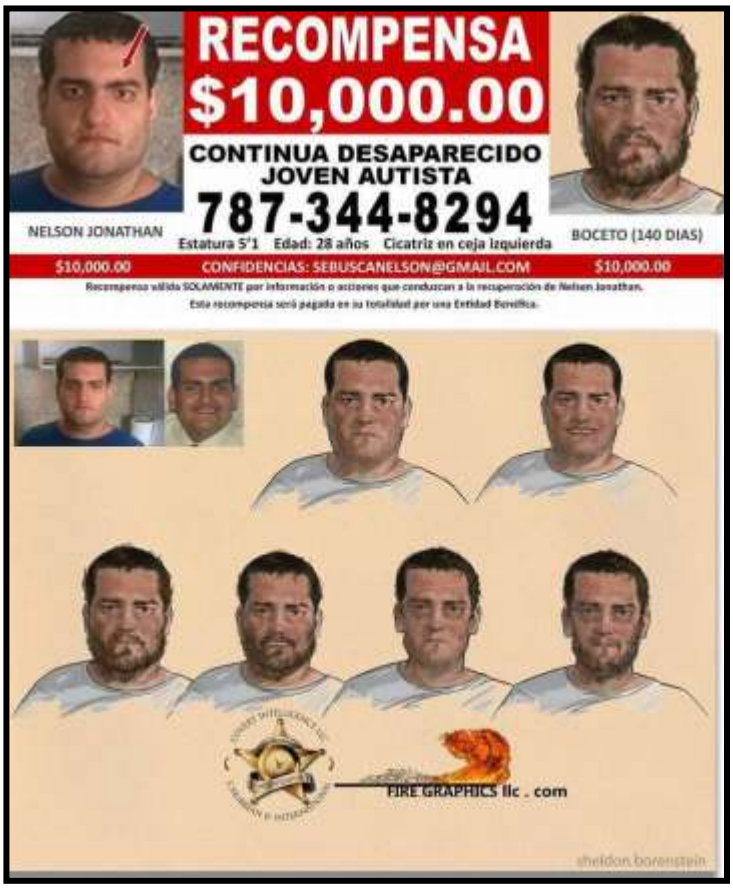
Congratulations Nicole

*Intellenet member **Nicole Bocra Gray** was elected to replace Bruce as the representative of the investigative profession on the IASIR board of directors at the conference in Scottsdale.*

called upon his colleagues in the industry to produce a 3D sketch of how Nelson Jonathan would look like in the months after he got lost and developed a technique to make the image and related ads go viral, reaching as many people as possible.

During the following months, Fernández used that methodology to help families who were desperately looking for their missing loved ones, in the midst of suffering from lack of water, power, and basic communications as a result of the storm. Of the first seven cases, five were solved in less than a month, one of them within the first 48 hours. One who unfortunately remains missing is Nelson Jonathan Martínez, a young man with autism who got lost a couple of days after the storm. At right is a missing person poster with augmented sketches of how he might look now.

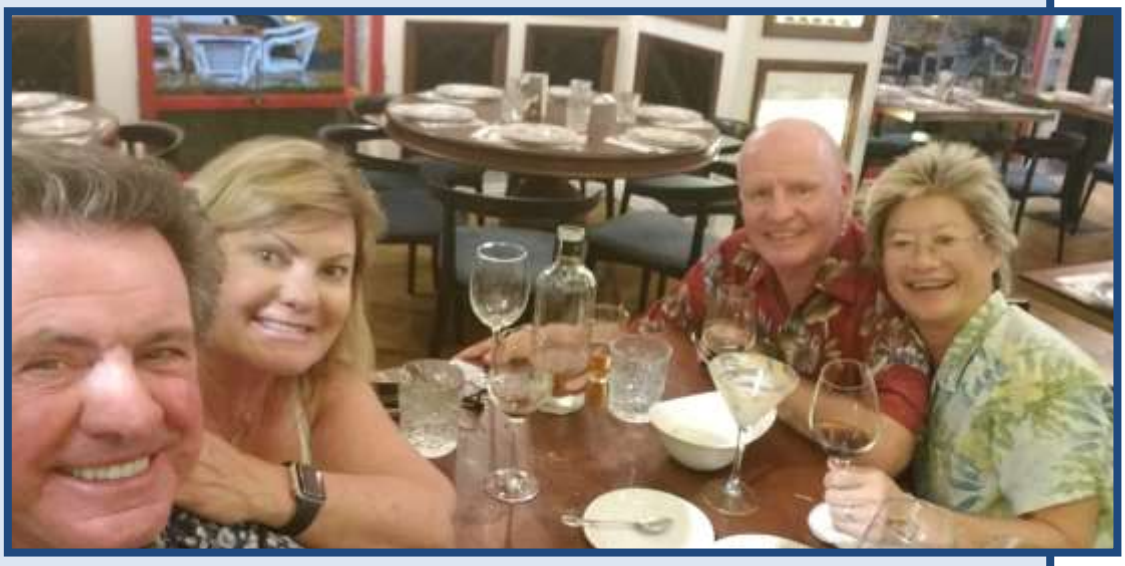
Fernández is now training other investigators and people involved with search and rescue in the use of his Viral Investigative Methodology through seminars and low-cost workshops. Meanwhile, he continues to help families of missing persons free of charge.



♦♦♦

Intellenet Friends Celebrate in Spain

During a vacation to Europe **Jim and Julie Zimmer** (in photo at left) enjoyed a visit with **Phil and Yin Johnson** while in Spain. Jim owns Benchmark Investigations in San Juan Capistrano, California and Phil and Yin own JJ Associates International in West Yorkshire, United Kingdom.



The Internet—Today's Yellow Pages

by

William F. Blake, CPP, CFE

Historically, to locate a particular product or service, the consumer consulted the classified ads (Yellow Pages) of the telephone directory disseminated by the local telephone company. As we move further into the 21st Century, telephone books are disappearing in favor of Internet advertising. This form of advertising requires that a website be available to identify the products and services a business has to offer.

While the requirement for a website is acknowledged by many businesses, some do not have a website and lose this valuable marketing tool. A check of 399 private investigation agencies in an eastern state revealed that 277 businesses (57%) did not have a website. Some agencies that had websites did not have a professional appearance and did not adequately identify their services.

Some of common deficiencies included one or more of the following:

- The print font was too small to be easily read.
- The colors used did not provide sufficient contrast for easy reading; i.e., gray on black.
- A complete contact listing was not available.
- Some website language was in the vernacular and not professional in appearance.
- The agency title did not present a professional name; i.e., "Got Cha Investigations," "Gumshoe Investigations," "Dead to Rights Investigations," "You Ask, I Find Them," etc.
- Some of the listing had information that was more appropriate for a family history website than a private investigation agency; i.e., "I worked in a farmer's field while I was in grade school," "My dog is named Ralph," "My father was in law enforcement for many years," etc.
- Some websites had large photos of their staff, from the owner of the agency to the file clerk with no explanation of how they contributed to the agency operation and were in fact, of no value.
- The qualifications of agency personnel were not outlined in specific terms; i.e., "Joe is an experienced investigator," "I have worked with Joe for many years." The extent of investigative experience is not stated, and it is not known if the individual is a neophyte or very experienced investigator.
- When an individual is seeking an investigator for a domestic issue, the inclusion on the website of a lengthy article with photos entitled "What is a cheating spouse?" is inappropriate and not necessary as the person seeking assistance probably is aware of such information.
- The "Contact Us" section should include a complete address, telephone number and e-mail address. Some websites include an e-mail form for completion but can be a "turn-off" for some people with limited computer literacy.
- It is superfluous to include the names of the crimes and situations investigated by the agency when it is assumed that the word "investigation or investigator" does not limit the scope of investigative activity.

Your agency website is a primary marketing tool for your business. The website quality is also an indicator or your professionalism. Maximum effort should be put into developing your website as its quality is also an indicator of your work quality. The do-it-yourself website is not always a good investment as many of them lack necessary features and evidence of professionalism.

Bill Blake is owner of Blake and Associates, Inc. in Highlands Ranch, Colorado. He can be reached at (303) 683-3327 or billblake2@aol.com.

♦♦♦

ISPLA Insights for INTELLENET

by

Bruce H. Hulme, CFE, BAI

ISPLA Director of Government Affairs

Since the 2018 mid-term elections, very little federal legislative action occurred on the part of Congress; although a farm bill was recently passed and a temporary government shutdown looms over funding of a border wall. Regarding the 2018 elections, ISPLA-PAC did not contribute to any candidate, notwithstanding it was the only national investigative and security professional association to make a federal political action committee donation to a federal candidate in 2017. However, as ISPLA-PAC's treasurer and ISPLA's government affairs director, I continue to keep abreast of the latest decisions and trends regarding federal election law. Should INTELLENET members wish to financially contribute to ISPLA's lobbying efforts, checks may be mailed to ISPLA at: 235 N. Pine Street, Lansing, Michigan 48933. If contributing to ISPLA-PAC donations must be made by PERSONAL check only. Thank you!

To contribute to ISPLA's lobbying efforts, please mail checks to ISPLA at: 235 N. Pine Street, Lansing, Michigan 48933. If contributing to ISPLA-PAC donations must be made by PERSONAL check only. Thank you!

Two FEC recent decisions below -- an Advisory Opinion and a Matters Under Review -- are worth noting. Also in this article are comments on security data breach state and federal legislation that will affect our profession's continued access to various databases we utilize, "Ban-the-Box", GPS and criminal defense issues to be addressed in the upcoming term of the U.S. Supreme Court.

Federal Election Advisory Opinion Issued

On September 6, 2018, the Federal Election Commission approved an advisory opinion (AO 2018-11) in response to a request from Microsoft Corporation. The Commission concluded that the requestor's proposal to offer a package of enhanced online account security services to its election-sensitive customers, at no additional charge and on a nonpartisan basis, would not result in the making of a prohibited in-kind contribution because Microsoft would be providing such services based on commercial and not political considerations, in the ordinary course of business, and not merely for promotional consideration or to generate goodwill. Thus, the Commission concluded that the proposal is permissible under the Federal Election Campaign Act of 1971, as amended (the Act), and Commission regulations. The Commission also noted that Microsoft's services would further the Commission's implementation of the ban on foreign participation in elections at 52 USC §30121.

Matters Under Review Before The Federal Election Commission: In the Matter of Donald J. Trump for President, Inc. and Timothy Jost in his official capacity as treasurer; and Donald J. Trump

The complainants were the Campaign Legal Center, J. Gerald Hebert, Democracy 21, Paul S. Ryan, Fred Wertheimer, Michael Glenn Bradley, and the American

Democracy Legal Fund. They alleged that Donald J. Trump and his campaign committee and treasurer Timothy Jost knowingly solicited contributions from foreign nationals in connection with his 2016 presidential election by sending emails to members of foreign parliaments in June and July 2016. The FEC closed its file on September 6, 2018 (MURs 7094, 7096, & 7098). While the Commission has publicly committed to prioritizing complaints regarding foreign national contributions, according to the vice-chair Republican members appeared to dismiss any Trump related FEC matters. Earlier this summer, they refused to investigate whether President Trump converted campaign funds to personal use by using campaign funds to promote his own financial interests and appear to have little interest in pursuing alleged violations of the law by the Trump Committee, under any circumstances.

Data Breaches & Privacy Issues

The General Data Protection Regulation (GDPR) now in force among European Union country members, among other provisions, mandates that companies notify data-holders of a breach within 72 hours. It also gives E.U. residents the "right to be forgotten" by having their data wiped off a company's servers. In the U.S., there is no comparable federal law that governs how all states handle data breaches and protects consumers' information. As it stands now, each of the states have different breach notification requirements, but the majority do not have sweeping legislation on the books on how companies handle personal data.

Facebook Faces $1.63 Billion Fine - Test of GDPR Sanctions...

As much as a $1.63 billion fine by the EU under the provisions of the GDPR for Facebook's recent data beach wherein hackers again compromised the accounts of some 50 million users may be imposed if regulators determine it violated provisions of the EU's new privacy law. In the U.S. efforts are underway to replicate here aspects of the GDPR. Should regulators establish that Facebook violated the EU privacy regulations stiff penalties are likely. Ireland's Data Protection Commission, the lead regulator in Europe, has demanded Facebook provide additional information about the nature and scale of their breach and the identity of Europeans affected by it.

One recent effort at creating a national data privacy law here comes from U.S. Rep. Hank Johnson, D-04-GA, Ranking Member of the House Judiciary Subcommittee on Courts, Intellectual Property and the Internet, who on July 26 introduced two bipartisan two bills.

H.R. 6547, the Application Privacy, Protection and Security Act of 2018 (APPS Act) ...

This measure is meant to govern the use of personal data on mobile devices. Smart phones and apps have tremendous benefits that enrich consumers and society. The mobile economy is also one of the fastest growing industries in the world, and big data is commonly referred to as the new oil. But this rampant growth also presents novel and unique challenges. Mobile apps collect highly personal information like contact lists, photos, texts, location, and calendar items. These apps often access data like messages or contacts without consumers' permission.

The Pew Research Center has found that the vast majority of Americans want control over their personal information, but only 9 percent believe that they have this control.

"Every day, more companies are looking to mobile as the future of media," Congressman Johnson noted, "Bridging the 'digital divide' means building protections into the technologies that we use, and to do that, we need privacy legislation that works for us, the consumer."

The APPS Act will boost consumer privacy on mobile devices by requiring app developers to maintain privacy policies, obtain consent from consumers before collecting data, and securely maintain the data that they collect. We all have the right to protect our personal information and companies must adopt responsible and transparent data use policies.

The APPS Act would give consumers the tools needed to help protect their online privacy and grew out of Rep. Johnson's APPRights initiative, a web-based legislative project launched in July 2012. This project opened a public conversation about how Congress might help ensure the privacy and security of mobile device users. Amidst the growing clamor for federal action to safeguard consumers' privacy and security, Rep. Johnson used

this initiative for his legislation to better protect app users' rights. He also worked closely with developers and stakeholders to ensure the APPS Act protects consumers without disrupting functionality or innovation through the APPS Act's safe harbor provisions.

H.R. 6548, the DATA Act of 2018, Empowering Consumers to Access, Correct, and Opt-Out of Big Data Collection and Use ...

This measure would allow U.S. citizens to have their data erased from corporate servers, and would make it easier for consumers to opt out of having their data used by third-party collectors. Aspect of these bills, if enacted, could affect information data brokers and professional investigators. Rep. Johnson believes his bills did not pick up traction in the past because of an anti-regulatory environment in Congress. However, he said that because of the recent high-profile data breaches, they may be more likely to pass this time around and provide uniform rules for all 50 states. "It makes sense that there be a national standard as opposed to up to 50 different standards. This is a matter of the interstate commerce clause. It's a classic situation for federal government to set down a uniform policy that provides guidance for those commercially involved and for consumer interest." The Facebook-Cambridge Analytica scandal exposed earlier this year, in which data of another 50 million users was collected and used for election purposes, showed consumers lacked even basic protections for their data online. Congressman Johnson contends his legislation would deliver critical updates and modernization of our digital privacy laws stating, "Privacy is an issue that should unite us, not drive us apart. We have fully entered the era of big data, and consumers access the Internet through mobile devices now more than ever. It's past time our laws reflect this reality through common-sense rules for data collection, transparency, and use."

Consumers Want Notice and Choice in Regards to How Data Is Collected, Shared and Used-- And to Implement Secure Protection Standards ...

A study in July by Kapersky Lab shows the percentage of consumers who are now more concerned about the collection of their personal data is up sharply from 2016. According to the study, more than 60 percent of consumers are "uncomfortable with sharing their location information with websites and applications – up from 39 percent in 2016." Furthermore, over half of people (56%) are very concerned that someone could see everything they do or watch on their device through an app. A similar percentage (50%) fear that someone could physically track them down using geolocation information from their device."

Consumers are increasingly connected through smart devices, while data continues to drive business practices. The Federal Trade Commission (FTC) recently noted in a report that this is "the era of big data." What follows are some comments that privacy advocates will espouse and that the private investigation and security professions will need to be prepared to address.

Many have raised concerns, however, that this data may harm low-income and underserved communities, particularly minorities. Wade Henderson, the President of the Leadership Conference on Civil and Human Rights, noted in 2014, "Big data has supercharged the potential for discrimination by corporations and the government in ways that victims don't even see." A former FTC Chairwoman Edith Ramirez has likewise observed that "the same analytic power that makes it easier to predict the outbreak of a virus, identify who is likely to suffer a heart attack, or improve the delivery of social services, also has the capacity to reinforce disadvantages faced by low-income and underserved communities," including price and customer service discrimination.

With these concerns in mind, it is critical that consumers -- particularly low-income and minority populations -- have access to the troves of data collected about them, the ability to correct false information, and the right

opt-out of data collection for marketing purposes.

"Consumers should have access to the volumes of personal data collected about them," said Johnson," "And more importantly, we should all be able to correct false information before losing access to potential employment, insurance, housing, or credit opportunities."

The Data Act would bring big data out of the shadows, create transparency and control for consumers over their personal data, and provide consumers with the tools to correct the record and minimize collection.

California Consumer Privacy Act of 2018 to Become Effective January 1, 2020

The information that follows may not necessarily have an initial impact on every investigative and security professional, nor will the European Union's recently enacted General Data Protection Act (GDPR). However, the two measures will influence aspects of future federal legislation as public awareness of privacy breaches increases. They will also promote future federal legislation to increase restrictions against the sale and acquisition of personal information without consent of the individual and will require that consumers have the opportunity to opt-out.

On June 28, 2018, California enacted a hastily drafted and ill-conceived data privacy law after only one week of work. Unless AB 375, the California Consumer Privacy Act of 2018 (CCPA) is amended before its January 2, 2020 effective date, the law will become the strictest data privacy law in the U.S. The measure will require data privacy protections and requirements similar or broader than imposed in the European Union's General Data Protection Act (GDPR), that became effective on May 25, 2018. That state's legislature acted expeditiously to avoid a citizens' initiative being pushed by "Californians for Data Privacy" from appearing on the 2018 November ballot. Passage of California's AB 375 caused the initiative to be withdrawn from the ballot, thus buying time to review and amend the new law before its effective 2020 date.

The law affects for-profit businesses that do business in California and either have annual gross revenue of $25 million or more; collects, sells or shares for commercial purposes the personal information of at least 50,000 consumers, households or devices; or derives at least 50% of its annual revenues from selling consumers' personal information. This law also applies to co-branded business entities that meet the forgoing criteria, even if he affiliate conducts no business in California.

Transparency of Data Collection

Similar to the EU's GDPR, business entities that sell or collect personal date on residents of California will be required to provide such individuals information about:

- The categories and specific pieces of personal data that the business has collected or sold,
- The categories of sources from which such date was collected,
- How the data will be used, and
- To whom the data will be disclosed.

Businesses will also have to identify at the time of data collection the personal data that is being collected and how it will be used. Once the individual's personal data has been collected, such information may not be used for a different purpose without notifying the individual. Where technically feasible, the business will be required to provide a copy of the collected data to the individual in a portable format. However, there are limited exceptions for personal data that is collected for a single, one-time transaction, if the information is not sold, retained, re-identify or link the data.

Right to Be Forgotten

Unless an exception is applicable, a business must delete the personal data on the request of a California resident. Exceptions for retaining data that is necessary for the business include:

- To complete the transaction for which the data was collected;
- Detect or protect against security incidents or illegal activity, or to prosecute persons responsible for such illegal activity;
- Identify and repair errors that impair intended functionality;
- Comply with laws or legal obligations.

Notice and Opt-Out

A business that collects or buys personal data of a California resident cannot resell that information to a third-party unless the individual has received notice of the proposed sale and an opportunity to opt-out. More restrictive measures are imposed if the data relates to children under the age of 16.

Additional Limitations

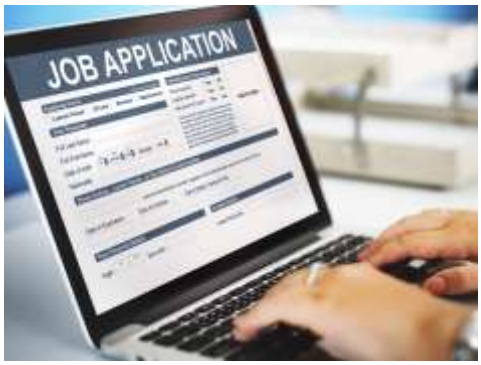
A business cannot refuse to provide goods or services to individuals who exercise their privacy rights. However, the business *can* charge different prices or provide different levels of service to individuals based on their privacy selections, but only to the extent that the difference is "reasonably related to" the value provided by the individual's data.

If the business offers financial incentives for consumers to provide personal data, the business must notify individuals of financial incentives, the consumer must expressly opt-in to the program, and the consumer must be able to opt-out at any time.

"Ban the Box" Legislation Gains Steam

Thirty-one states and more than 150 cities and counties in the U.S. have adopted the "ban the box" laws that aim to eliminate the stigma associated with a criminal conviction. The National Employment Law Project has estimated that nearly three-fourths of the country lives in a jurisdiction that has a rule restricting how companies can use criminal background checks as part of the hiring process.

Advocates contend questions about a candidate's criminal background create a bias against those applicants. Some employee advocates contend various laws do not go far enough in terms of enforcement. Management-side lawyers have argued the laws could place undue burdens on employers.



The New York law is one of dozens in states and cities around the country that restrict companies from asking job applicants about criminal records, particularly early in the application process. The law, on the books since 2015, requires employers to individually assess an applicant's criminal record and determine its relevance before rejecting the would-be employee. New York City has a similar ordinance. Massachusetts also enforced its law for the first time recently.

Aldo Group Inc. came under scrutiny in New York after an undercover investigator discovered that not only did the store's job application include a question about criminal background but a hiring manager reportedly said any candidate with a felony would not be considered.

These criteria, in addition to the alleged dissemination of information to hiring managers that felons need not apply, resulted in a fine from the New York Attorney General's Office in June, the latest in a string of enforcement actions from that office. The international retailer of handbags and accessories paid $120,000, one of five recent New York attorney general settlements involving alleged violations of so-called "ban the box" regulations. The settlement also required the company to take steps to comply with state laws that prohibit discrimination against job applicants with criminal records. The New York Attorney General's Office has also entered into agreements with Bed Bath & Beyond, Big Lots Stores, Inc., Marshalls, and Party City retail outlets.

Aldo, with 53 stores across New York state, said in a statement it has not conducted or used criminal background checks in its hiring process since 2015. It said the investigation revealed that New York state stores were distributing outdated applications, without the knowledge of the human resources team. Aldo said it updated its forms, pulled them from stores and circulated an updated application.

"The Aldo Group does not conduct criminal background checks or consider criminal background information in its hiring process, and is not aware of any applicant in the state of New York who was denied employment on that basis," the company said in a statement. "While the company is in disagreement with most of the New York attorney general's findings, there is

always more that an employer can do to ensure that it remains compliant."

Lessons for Employers

Many multistate-employers have eliminated across the board a criminal background question on job applications.

"We have reached a place where there are so many ban-the-box laws throughout the United states, it's become a very large minority," said Joe Schmitt, a labor and employment shareholder at Nilan Johnson Lewis in Minnesota. "I flipped in the last two years—I used to tell clients to comply piecemeal and have a box and eliminate for others. Now, I say create a uniform policy avoiding the question."

Despite the prevalence of state and local "ban the box" laws, there haven't been significant court cases to date, Schmitt said. New York in particular, he said, has been aggressive in its enforcement.

The agency's claims against Aldo showed one potential pitfall for companies—how much discretion managers have in the hiring process. "The New York attorney general is attacking Aldo on the grounds it provided too much discretion to people in the field to allow them to making decisions, as opposed to establishing strict guidelines," Schmitt said. "The argument is that this leads to discrimination."

GPS Devices Banned for Troops on Deployment

Deployed U.S. military service members will no longer be allowed to use fitness tracking apps or other wearable technology such as Fitbits and iWatches that rely on geolocation, according new Pentagon policy.

According to an August 3, press release, Deputy Secretary of Defense Oatrrick Shanahan wrote: "The rapidly evolving market of devices, applications, and services with geolocation capabilities presents a significant risk to the Department of Defense (DoD) personnel on and off duty, and to our military operations globally....These geolocation capabilities can expose personal information, locations, routines, numbers of DoD personnel and increased risk to the joint force and mission." The discovery that geolocation capabilities can expose locations of bases and important facilities based on where the geo-tracking stops prompted this policy change.

Data firm Strava's January 2018 release of a heat map revealed the locations and pathways of military installations around the globe due to user data on fitness apps such as Polar Flow. The global map reflected more than 1 billion paths that the Strava app tracked, but patterns and locations of U.S. service members could be garnered from zooming in on sensitive or secured areas.

The new policy does not require a total ban and only affects service members at operational bases or locations. Personnel working at the Pentagon will still be allowed to use the devices. There are no prohibitions ob members of the military from having the devices with them when they deploy, as long as the geolocation services are disabled. Each on-site commander will have final say as to what devices they will allow.

In some cases, the geolocation services will be allowed to be turned on after a security review has been conducted.

Criminal Defense: U.S. Supreme Court Calendar

Two Case Comments from Dean Erwin Chemersky, University of California at Berkeley School of Law

Double Jeopardy: SCOTUS "Stare Decisis" Federalism Issues to Be Heard

In Gamble v. United States, the U.S. Supreme Court will consider whether to overrule the "separate sovereigns doctrine," which provides that the federal government and state governments are separate sovereigns, and double jeopardy does not bar prosecutions against the same person for the same crime in both federal and state courts. This was the holding in Abbate v. United States (1959) and Bartkus v. Illinois (1959), though the doctrine can be traced to Supreme Court decisions going back to the middle of the 19th century.

Most recently, in Puerto Rico v. Sanchez Valle (2016), the court held that the United States and Puerto Rico are not separate sovereigns for purposes of double jeopardy. But Justice Ruth Bader Ginsburg, in a concurring opinion joined by Justice Clarence Thomas, urged the court to reconsider

the separate sovereigns doctrine.

The court granted review in Gamble to do just that. Terance Gamble was convicted in Alabama in 2008 of second-degree robbery. In 2015, as a result of a traffic stop, he was found to have a gun, which violated both state and federal laws preventing a felon from being in possession of a firearm. He was convicted in state court and sentenced to a year in prison. Gamble also was indicted in federal court and entered a conditional guilty plea after the district court rejected his argument that this was impermissible double jeopardy. His federal sentence is 46 months, or almost three years longer than the state court sentence. The issue before the court is simply "whether the court should overrule the 'separate sovereigns' exception to the double jeopardy clause."

Death Penalty - Eighth Amendment

In Madison v. Alabama, the Supreme Court will consider whether it is cruel and unusual punishment for a state to execute a person who has developed severe dementia and is unable to remember his offense. The court previously ruled that it violates the Eighth Amendment for a state to execute the mentally insane—Ford v. Wainwright (1986); Panetti v. Quarterman (2007)—or the mentally disabled— Atkins v. Virginia (2002). The question is how this applies to a prisoner who has developed dementia, something courts will increasingly face with an aging population on death row across the country.

In Bucklew v. Precythe, the court will consider whether it is cruel and unusual punishment to use a method of execution, lethal injection, that risks great pain and suffering because of a rare medical condition. In Baze v. Rees (2008) and Glossip v. Gross (2015), the court rejected facial challenges to laws that provided for execution by lethal injection. Bucklew v. Precythe is an as applied challenge based on Bucklew's rare and severe medical condition. ♦♦♦

Bruce can be reached at BruceHulme@yahoo.com.

Our 36th Annual INTELLENET Conference will be held at the Charlotte Marriott City Center hotel located at 100 West Trade Street, Charlotte, NC 28202 from April 2-5, 2019. Our local hosts, Don and Gina Hubbard, are hard at work with the conference committee planning another fabulous training and networking event you won't want to miss!

36th Annual INTELLENET Conference

Charlotte, NC | April 2—5, 2019

Make your Charlotte Marriott City Center hotel group rate hotel reservation now!

Our group room rate is $159.00 per night and is available from March 31 – April 7, 2019.