INTELLENET *News*

Official Newsletter of the International Intelligence Network, Ltd.

Intellenetwork.org *Fall 2013*

In this issue. . .

Dear Intellenet Members:

Intellenet continues to improve each day, and helping members obtain work is one of our main goals. Are you aware of Intellenet's "initiatives" program?

Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet

I hope each of you had a very productive and enjoyable summer. As I have been speaking to members from all over, I have found that many of you are extremely busy with work, which is great to hear. But some areas of the economy have seen slower growth in work opportunities. Helping members obtain more work is what our "initiatives" program is all about.

The initiatives program is about obtaining bigger clients, for investigations and security operations nationally and internationally. The program helps the entire membership, because individual members are the ones who perform the investigations for not only an existing client (one of yours, for example) but for potential new clients who have learned about Intellenet and its international reach. That is exactly what has happened in the 11 programs that we have been involved with so far. Close to 300 members have participated in one aspect or another in these programs, which to date have seen billings of approximately one million dollars. I know of no other association with the ability to facilitate such a program. Our mandated minimum 10 years individual investigative experience, our membership vetting process and our high ethical standards play a significant part in securing an initiative engagement.

"You can increase your billable time and assist others by searching for initiatives..."

I. *There are two ways to participate in this program:*

a. **Obtaining the client.** When you find a prospective client, Intellenet can help with a RFP and show the client the benefit you bring with the *global* reach of being associated with Intellenet. If you are unsure or nervous about how to approach a prospective client, contact us for some advice. We now have a history of experience doing this and there are Intellenet members willing to share their own experiences. If you are able to obtain a client it remains *your* client. Intellenet does not have any control over your client relationships nor do we want to. We are just the support mechanism.

b. **Providing the resource**. Having an investigative resource in a needed area is key to the program's success. But we have to know you are there and can provide that resource.

II. *How are members used in these programs as a local resource?*

a. As noted, an important aspect of the program is having a member in the needed location. This basic requirement has worked well and is a big reason we do not over saturate areas with members, which provides a higher opportunity for each member in a needed location. You are where you are, so when a prospective client needs something we need to know you can provide that particular service or resource.

b. We need your one page resume on file with Intellenet. This has been communicated numerous times by Jim on the list serve. Each client has different needs and wants, including different requirements or credentials from a service provider. These may or may not include a college degree; ability to speak a specific foreign language; provide contract guards; license to carry a weapon; or hands on experience in a specific career field or subject matter. Having your one page resume on file helps ensure an opportunity if your credentials and/or background meet the needs of the client. If you have had any major changes to your professional resume make sure you send us an update.

Continued on next page…
►►►

Continued from Peter's Posting…

How can you help our initiatives program? You can increase your billable time and assist others by searching for opportunities for initiatives, and by recommending new members where we have geographical needs. Shortly, we will announce requirements for new members in both U.S. and international locations.

I hope to see many of you in Puerto Rico next year. Do not hesitate to contact me regarding your questions, comments or concerns. You can reach me at peter@ewiassociates.com, phone (734) 320-9240.

All the best to you and yours this fall season.

♦♦♦

What is Wintellenet?

By Robert Dudash
Director of Operations

Often times, members share tidbits of information with me or call me to check on rumors.

Recently I was asked, "Is Intellenet changing its name?" The individual – *with tongue firmly in cheek* -- said he had heard Intellenet was thinking about changing its name to *Wintellenet*, and he went on to provide an explanation. His call was in response to the *Initiatives Program* implemented by Founder and Executive Director Emeritus Jim Carino and now carried forward by Peter Psarouthakis with Jim's assistance.

The individual was highly supportive of the program and boasted that only Intellenet had such a program. Why did this individual wonder if Intellenet would now be known as *Wintellenet*? As we have heard many times over the years, there is no "I" in team and since Intellenet is the consummate "team," the thought was to add the "W" before the "I"! We could then be *Wintellenet*, because we are a professional, resourceful and effective team.

If you want to be a part of our initiatives program, it is essential for you, if you have not already done so, to forward a one-page resume detailing your unique qualifications as an investigator or security consultant. Jim has sent numerous requests for this resume, but, amazingly, not nearly all our members have responded. If you have not done so and want to be part of our initiatives program, please send your resume to intelnet@verizon.net. See the sidebar on how to construct your one-page resume. *If you've already sent a one-page resume, please do not send another one, unless it needs updating.*

Intellenet has been identified as the premiere investigative association and membership is a privilege, not a guarantee. *We are a team*. We are all interested in being successful in our endeavors and ensuring we set and maintain the highest professional standards possible. We are unique in that our senior leader had a vision and followed through on that vision which, in effect, has provided our members with the ability to seek out and develop programs which provide billable time, for one's self and other members as well.

Of course, we don't need to change our name. That brand is well established. ♦♦♦

Your "Initiatives" Resume

In addition to your contact information, the one-page resume should include:

- PROFESSIONAL EXPERIENCE: Number of years of progressive responsibility in investigative and/or security experience; broken down by government agency, military, private sector, etc.
- SPECIAL EXPERTISE: Limited this to four categories, for example; school security; financial crimes; hostage negotiation, computer forensics, etc.
- EDUCATION: List college or university degrees.
- TRAINING: List special programs and professional certifications.
- PROFESSIONAL ASSOCIATIONS: Limit to five, with Intellenet as the last one.
- NOTABLE ACCOMPLISHMENTS: Limit to five; include published works, awards and honors, etc.

●●●

Professional Development: It Takes a Village

An Initiative for Intellenet Members

By Barbara W. Thompson and Jeff Stein

A lot of people use the terms "continuing education" and "professional development" interchangeably, as if all there is to professional development is to continually take courses.

Notice that we said "take courses" and not "to learn." Many states require a certain number of continuing education credits in order to maintain a private investigator's license, and license holders in those states dutifully sit for the requisite number of hours and listen to someone who may or may not know as much as the student does about the topic at hand. Do that enough and, bingo, they have satisfied their hourly requirement and the licensing agency pronounces them qualified to go forth and deal with the public. Or maybe the instructor is talking about something the investigator needs and wants to know, but the investigator doesn't have the background yet to understand at the level at which the speaker is teaching. Some states have no continuing education requirement, but serious investigators know that it is essential to keep up with changes in the law, with technological developments, and other investigative techniques critical to providing outstanding services for their clients.

In fact, the Intellenet paradigm is so successful we thought that with a little tweaking — and extraordinary hubris on our part — it might be improved.

So, for purposes of this article, let's stipulate that continuing education is at least a part of professional development. But professional development is so very much more.

When you first opened your practice, did you have the skills and knowledge necessary to provide either the general or niche services you intended? For those of us whose private investigative business is a second or third career, the answer is probably yes -- for the most part. But when your first case came along, did you have any questions about how to proceed? Or perhaps you had technical or strategic questions that weren't so easily answered in the private sector as in your previous law enforcement or military career? Did you come from a commercial security background? Were you able to land on your feet with all the answers to all the questions that actually arose when the work became real? What about (shudder) ethics and proper conduct?

Or, maybe you opened your doors, had the telephone hooked up, put up a killer website, advertised in the telephone directory, but you just weren't generating the work load that you wanted as fast as you wanted?

Those of you who are in private practice for more than five years, especially through the recent "Great Recession," probably did the sensible thing when you first started out. You networked. You probably had friends from your previous career who started their private practices before you and could offer you advice. And then those friends introduced you to other friends and so on, until you had built a solid network of professionals that you could depend on for "just in time" advice and assistance related to a specific issue.

It really does take a village...

The authors of this article were fortunate enough to have identified and been accepted by some of the most remarkable mentors in the investigative field. We joined our state association and became active in it, eventually holding several board positions. The network grew with almost no effort on our part. Intellenet was one of the networks we were admitted into and the return on investment was and still is overwhelming.

In fact, the Intellenet paradigm is so successful we thought that with a little tweaking – and extraordinary hubris on our part -- it might be improved. These improvements have now been brought forth in the Society for Professional Development, LLC (SPD).

Continued on next page ...

The concept for SPD was conceived as a result of a minor, but frustrating, detail in the Intellenet rules. Specifically, when someone asks a question, the responses are sent only to the inquirer and not to the list as a whole. So the membership never gets to read the answer.[(1)]

The Ideal Professional Association …

So, about five or so years ago, we started pondering what the ideal association of professionals would look like. This is what we came up with; it would offer:

- Some sort of communication vehicle other than a list serve to generate conversations among members;
- A knowledge base that members can consult when they have questions that have already been answered;
- A medium for members with specific interests to interact with each other;
- A mentoring system in which members with questions related to real cases can *confidentially* ask true experts in specific fields (even outside private investigations) for assistance, and a way for the mentor and mentee to establish a consultative agreement if it is deemed necessary;

- A medium for members who wish to submit news articles, white papers or other scholarly works for use or purchase by other members (also a marketing tool);
- A solid formal continuing education program presented by true experts which will be advertised as appropriate for learners with various experiential backgrounds (introductory, experienced, or advanced); and
- *A way for the members to make themselves known to potential clients. We became most excited about this element.*

How many times have you been to classes put on by various experts in marketing and come away with the feeling that those strategies won't work for you? You aren't comfortable cold calling potential clients, or sending out mailings. You're just not into mingling in large groups. Some people are more comfortable marketing their services by speaking about the topics they know and then letting word of mouth take over. You aren't the only person who might feel more comfortable telling people what you can do in a "natural" way.

Who are investigators' potential clients?

Of course, anyone is a potential client, but for the most part, we primarily work for lawyers, accountants, businesses and governmental agencies. These potential clients need continuing education and professional development also. They should be included among the membership of SPD and can also be invited to speak, become members, and become experts in their field of endeavor.

So, built right into the basic concept of SPD, investigators and potential clients are rubbing elbows, asking each other for advice, forming consultative relationships and making referrals. Investigators may find built-in legal and accounting advice from fellow members. An investigator who is interested in expanding into litigation support can get advice not only from other investigators who have more experience, but also from the lawyers whose needs the investigators will be meeting. And it all starts from, *"Does anybody know about _____?"* and *"Sure, I've been doing that for 20 years."*

The SPD Initiative …

So, here's the initiative part. This business plan won't work without experienced experts, and the absolute ultimate place to go for investigative talent is Intellenet. SPD needs presenters, writers and people to evaluate presentations in their area of expertise. We need people who

Continued …

(I) Now, we're not suggesting this rule should be changed. There are several hundred good reasons for it and only the one we just mentioned works against it. Please do not interpret this as a plea for change. It is easy enough to request that the original seeker of information forward the responses to specified members, or summarize the responses for the group. These are very workable solutions, although it puts additional work on the person summarizing. Many thanks are due to the members who are accommodating enough to share in this way.

… see the value in extending a helping hand to other professionals in order to generate relationships that may just blossom into clients.

The Society for Professional Development is a for-profit company, and so are Intellenet members' companies. SPD's business plan calls for remuneration for presentations, for reviewing speakers' outlines and for published articles. After some market research we have found that currently webinars are more successful than physical seminars, so presenters will receive both an honorarium for the initial presentation, and then residuals for playbacks of their webinars. This allows speakers to prepare their presentations and deliver them without the time commitment and expense of travelling to distant locations. SPD is looking for one-hour seminars as well as courses in which multiple one-hour seminars will be required to cover a topic adequately. SPD is looking for any type of information that you'd like to provide that would be of interest and use to other investigators and/or investigators' potential clients. We're also looking for any advice that you'd care to give us about how to make SPD more useful to you.

Please visit our website at www.spd-education.org. For more information feel free to contact Barbara Thompson at thompson@spd-education.org or phone (610) 430-6352; or contact Jeff Stein at stein@spd-education.org or phone (610) 696-7799. At the website, if you hover over the Join Us tab, you'll see a drop down tab titled, A Special Welcome for Intellenet Members. Please note that membership fees will be waived for anyone who submits a presentation that SPD makes available to its members or the public.

Be a part of the village whose goal is total professional development. ♦♦♦

Barbara Thompson and Jeff Stein are Intellenet members.

Employee Conflict is Costly: Chump Change It's Not!

By Beville May

Conflict that winds up in court costs American companies millions every year. In fact, Fortune 200 companies' litigation costs averaged almost $115 million per year, according to a recent survey. That figure does *not* include payouts to plaintiffs.

Mediation Makes Sense -- Dollars & Cents!

Three quarters of the lawsuits companies face involve employment disputes of discrimination, harassment, wrongful discharge or retaliation. The price tag to defend such claims averages $75,000.

Claims can take 12-30 months to wend their way through the "discovery" process. Then 98.9% settle before trial. And in the rare event your case goes to trial, only one page out of 1,044 "discovered" will actually be used in court. Ouch - that is one pricey piece of paper!

Mediation, on the other hand, resolves claims like these in as little as *eight hours*. Yes, you read that right: hours — not months, days or years — and at a fraction of the cost as well. With a mediation resolve rate of 80% or more, mediation makes sense. Dollars and cents.

Choose mediation to resolve employee disputes in a fiscally sensible manner. Or, let your cases continue to kick around the courthouse. It's your call. Just remember this: litigation will cost 0.6% of your bottom line. Like I said, we're not talking chump change. You can bank on that!

♦♦♦

Beville May is an Intellenet member. Her company, Prevent Claims, LLC, is located in Exton, Pennsylvania. Beville provides expert testimony and litigation support services in employment law issues. She can be reached at Beville@PreventClaims.net, or phone (484) 886-6006. This article is excerpted from Beville's newsletter, with thanks!

Member News

Welcome New Members …

John HODA, Milford CT
John HOUSEMAN, St. Louis MO
Robert (Bob) RAHN, Monroe NY

These are our newest members since we last published. You should have seen their mention in one of Peter's *InfoBriefs.* If we missed a name in this issue, we apologize. Let us know and we'll mention you in the next issue. Welcome, Gentlemen, to the premiere network of investigative professionals and security specialists.

Congratulations to Karen Hewitt …

Karen Hewitt, Hewitt & Cowden Investigations, Inc., Colleyville, TX is now Assistant Director at the University of North Texas, at the school's Private Investigator Academy. Karen joined the academy's staff this past June.

Congratulations to John Sexton, CII's New President…

As this issue of Intellenet News was being prepared, **John Sexton, PPS, CST, CII** was being sworn in as the new president of the Council of International Investigators at its annual general meeting in Enniscorthy, County Wexford, Ireland. John is an executive protection specialist at Sexton Executive Security, Inc. in Fairfax, Virginia.

At our last count in mid-August, there were about 24 Intellenet members — who are also CII members — who planned to attend this conference. Not only will we have an Intellenet member as CII's new president, — who succeeds an Intellenet member, **Eddy Sigrist** — but one Intellenet member and his wife will be celebrating their 50th wedding anniversary while in Ireland at the CII AGM. A special congratulations is due to **Robert and Brenda Dudash** for what is a "really neat accomplishment," as Robert put it.

Two of Intellenet's own were presenters at FAPI's 2013 annual conference. **Jim Carino** and **Bill Blake** brought their pre-conference seminar, "The Role of the Private Investigator and Security Consultant in Negative Security Litigation," to the Hilton Orlando on September 26. Fore more on FAPI, go to MyFAPI.org.

Carrie Kerskie was a featured author in the newsletter of the Naples, Florida Chamber of Commerce in July. Carrie's article, "Identity Theft, Not Just a Risk for Individuals," highlights the challenges facing businesses in protecting not only their proprietary corporate information but also the information of their employees and clients. Carrie is president of Marcone Investigations in Naples, and a specialist in identity theft protection, detection and restoration.

♦♦♦

Guarding Services in Mexico

By Tom Cseh, Vance International Mexico

The United Mexican States is a federal republic consisting of 31 states and one Federal District (Mexico City). The federal cabinet-level Secretariat of Public Safety (SSP) governs private security company operations throughout Mexico. Additionally, each state and the Federal District have a public safety secretariat that exercises government oversight of state, municipal and private security operations in their respective states/jurisdictions.

In Mexico, the official work week for most employees in service industries, including private security, is a six-day work week or 48 hours. Overtime is calculated on all hours worked over eight hours a day, on public holidays and Sundays. The overtime rate is calculated at time and a half of the hourly rate.

Our guards and supervisors are paid above the minimum wage rate for private security personnel. They receive full medical benefits through the government-mandated Social Security system, life insurance and food stamps. A voluntary savings program is available with matching employer funds paid at the end of each year. In mid-year, company employees are, by law, entitled to a small percentage of the company's prior year's profit, when such is officially declared by corporate management and ratified by the Mexican Federal Tax Authority (SAT).

The federal license allows private security companies to conduct investigations and temporary/short term unarmed executive protection and custodial transport operations in all 32 jurisdictions. If a private security company is going to permanently station its personnel outside its principal operations area (i.e. a legal domicile), the company must obtain a current local state permit as soon as possible. Most state jurisdictions require a signed contract for providing guard services from the applying company and will not grant an operations permit until the

Continued on next page…

the private security company has all of its paperwork in order – an administrative process which might take 60 to 90 days to finish under ideal circumstances.

Both federal and state regulations require that all private security company personnel, including senior management and the administrative staff, undergo a background check that includes a query of police/penal records and a urinalysis test for drugs (usually every six months). A record of all security-related training is also required to be maintained.

Vance International does not have a permit for its personnel to carry weapons, which is also true of most private security companies operating in Mexico. Permission to carry weapons/firearms requires specific authorization from the Secretariat of National Defense (SEDENA) and authorization from the state jurisdiction where the security company is legally domiciled.

♦♦♦

Tom Cseh is Deputy Director of Vance International de Mexico, S.A. de C.V., an Andrews International Company, Mexico, D.F., Mexico, telephone 011-52-551-500-0400 (office), 011-52-1-554-353-1526 (mobile), email tom.cseh@andrewsinternational.com.

VANCE®
AN ANDREWS INTERNATIONAL COMPANY

Safety and Security Tips for Visitors to Mexico

by Tom Cseh, Vance International Mexico

1. Only drink bottled water when dining out. Tap water in most first class hotels is potable, but ask at reception desk if in doubt.
2. Eat food at roadside or sidewalk stands at your own risk. Amoebic dysentery, **E. coli** and **Salmonella** bacterial infections and even cholera are common food-related debilitating and, in some cases, life threatening diseases in Mexico City.
3. Usually at the end of the dry season (March – May and sometimes into early June), the Mexican Health Secretariat may issue food poisoning warnings involving consumption of any type of seafood. Bottom line – if you don't personally know the freshness of the catch or its refrigeration history – eat fish and shellfish (including shrimp) at your own risk.
4. Do not hail a taxi on the street – ever! Use the hotel taxi service, a taxi stand ("**sitio de taxi**") service or get the restaurant maitre d' or staff to get one for you.
5. Do not conduct meetings outside the office or hotel with persons unknown, especially when the meeting is requested by the latter at a place of their choosing.
6. Wear no flashy or expensive jewelry – even if fake. The common street criminals in Mexico City are usually stoned on drugs or alcohol - helps keep their nerve up and makes them more dangerous and unpredictable. Make yourself a less interesting, visible and desirable target.
7. Only use ATMs in the hotel or inside a shopping mall, and never one facing onto the street. Do not walk straight out onto the street after using it. Criminals often have surveillance on ATM's and watch for the first person to enter the street right after accessing the machines. You can now draw up to $6,000 pesos (about USD$500.00) in one daily transaction, so the criminals automatically assume they may have hit the jackpot when they zero in on someone they've seen just use the machines.
8. Avoid changing money at Mexico City's International Airport (AICM). Over the past 12 months, there have been several notorious cases involving foreigners changing money at established money exchanges inside the airport and then being assaulted several blocks away from the airport whether in an airport taxi or private conveyance. At least one fatality was reported when a French national resisted attempts by the assailants to rob him. It would always be better to change money at the hotel, but not going off the hotel property right after doing so.

Continued ...

Safety and Security Tips for Visitors to Mexico …

9. Be very careful when using your credit card to pay for merchandise in stores, for food in restaurants, hotel accommodations and car rental agencies. Credit card theft and cloning are rampant in Mexico and even the employees of legitimate enterprises have been known to be involved in such activities. Always have the salesperson execute the credit card transaction in your presence and do not let them carry your credit card away. Do not leave extra copies of signed credit card vouchers behind at the establishment. If you suspect that your credit card has been misused, contact the establishment management right away.

10. If walking out and about the town and someone unknown approaches and asks you a question, for example: **¿Tiene la hora?** (What time is it?) or **¿Sabe donde está….?** (Can you tell me where is….(or how to get to)….?) – **LOOK THEM BRIEFLY IN THE EYE; IGNORE THEM COMPLETELY or GIVE THEM A BRUSK "NO!"; AND KEEP WALKING AWAY FROM THEM – FAST!** These types of questions are common ruses to momentarily distract an unwary person while the assailant (or his partner – and there's almost always more than one of them) pulls a knife or gun in front of or behind the victim.

11. **"Splash & Grab"** pickpockets are back in fashion. When walking in a shopping mall or just out on the street watch out for anyone signaling to you that you have just been splashed from behind (or in front) with a mustard or ketchup-like gooey or runny liquid substance, especially when they offer to help clean you off in a nearby public restroom. While one or two persons may be enthusiastically helping clean your clothes, one of them will attempt to lift your wallet or purse or even just "fish" a couple of credit cards or cash out. Don't let anyone touch your clothing or get inside your "inner perimeter" and just move on as quickly as possible and clean yourself off later.

12. **For Men Only:** Avoid unknown or **shady "night spots."** They are typically used by **express kidnappers** to zero in on unsuspecting male customers. Female "escorts" are often used to entrap male customers in these areas. Drugged drinks to subdue victims are not uncommon.

13. **For Everyone:** If you intend to personally drive a rental or company vehicle while visiting Mexico City, please consider the following recommendations:

A. Obtain a **Guia Roji for "Ciudad de México,"** an up-to-date detailed map book of the city available in almost any bookstore and Sanborns Stores in particular. Using the Guia Roji, plot out all routes in advance and consider some alternate routes. Look for the small arrows on some roadways that indicate that the street might be one-way.

B. Ask someone in the hotel, usually the concierge, vehicle rental agency or someone in the office you are visiting for clear directions on how to get where you want to go **before** you actually leave. Get the address in writing and carry it with you, along with the phone number of the place if available. Do not stop in mid-travel to ask directions, even if you do get lost. Go to a gas station or a taxi stand and ask for new directions. **Do not seek assistance from the police.**

C. While traveling, be extremely vigilant around intersections with traffic lights, stop signs and speed bumps ("topes") for persons who might be waiting to assault you. Do not permit the windshield washer boys (and sometimes girls) to wash your windows. Do not argue with them either; look them briefly in the eye and merely wave them away with an index finger wag. Keep your eyes open for persons approaching from behind or along side the vehicle and watch their hands to see if they are carrying weapons or are hidden. Be prepared to take evasive driving action to get out of a potential ambush situation.

D. Leave sufficient space between your car and the vehicle in front of you that you can always see the rear tires of that vehicle touching the pavement. This will usually give you enough space to maneuver around that vehicle. Consider using the median strip even with a curb of up to even 12-18 inches high to escape. Turning your front wheels to a 45º angle and exerting maximum acceleration should be sufficient to jump

Continued...

Safety and Security Tips for Visitors to Mexico ...

jump the curb and continue over the median strip. Look between the trees or posts or other obstacles while traversing the median strip – the vehicle always goes where the eyes of the driver are looking! Even if your tire ruptures, keep driving – the vehicle will continue to run on its wheel rims until you finally brake to stop. **Keep driving until you are well out of harm's way!**

E. If someone hits your vehicle from behind, look in the rearview mirror or physically turn your head around to see who is in the vehicle behind you before getting out of your car to check the damage. If the operator of the other car is a woman or man driving alone, it may just be an innocent accident. However, if you cannot clearly see the vehicle or who is in it, do not get out of your vehicle and keep moving. If you see two men or more in the vehicle, do not get out of your vehicle and keep moving. Do not stop until you are in a safe area with lots of people around and in a well-lighted area if at night. Hitting a vehicle from behind is a common trick of carjackers and express kidnappers to immobilize their victim just long enough to take control of the situation. If there is any real damage to the rental vehicle because of the collision, just report it to the rental company as a "hit and run."

F. Always drive with all the car doors closed and locked and all windows up and locked. When the car is stopped in traffic at any location do not offer money to beggars on the street no matter how pleading they are. Look them briefly in the eye and then ignore them. Use the index finger wag if they persist. **Do not engage anyone approaching your car on the street in conversation – ever!**

G. Do not drive around with laptops, briefcases, purses, packages or other valuable items clearly visible on the seats of the vehicle. A common street crime in Mexico City is the typical "smash and grab" ("cristalazo"), where the criminal will break the window of the car to steal whatever he can get his hands on. Do not bother to physically chase the criminal if this happens to you! He will always have an escape route planned and may have accomplices available to impede a successful pursuit. **Better to store all valuable items in the trunk.**

H. If stopped by the police:

i. Do not leave the vehicle.

ii. Do not turn off the motor.

iii. Try to identify the uniform, badge and name of the policeman and make a note.

iv. Do not unlock your doors or windows and only lower the window no more than two inches if necessary because you have difficulty in hearing what the policeman has to say.

v. Even if you speak Spanish fluently, it is often better to feign ignorance and speak another language.

vi. Do not turn over any personal identification or vehicle documents to the policeman. Show them to him through the window glass only.

vii. Be courteous, but firm while trying to ascertain the nature of the stop. Do not accept the policeman's offer of a handshake and do not make insulting remarks to him either, no matter how angry or upset you are about the stop. **Note: It is a separate offense to insult a public official acting in the line of his or her duty.**

viii. Use a mobile phone to contact someone – even if faking it - and pretend to or actually call your embassy, office or family or company lawyer and advise that you are being stopped by a policeman for some unknown reason. If this is a bogus traffic stop on some fabricated or fictitious traffic violation, the police will usually back off if they see the person they stopped is contacting someone in authority. **Notes: (1) A driver using a mobile**

Continued...

Safety and Security Tips for Visitors to Mexico …

phone while the vehicle is in motion is committing a traffic violation in Mexico. (2) Do not automatically offer to pay a bribe to get out of a legitimate or fabricated traffic violation. Lately, both the policeman soliciting as well as the driver paying the bribe have been arrested by the municipal authorities trying to crack down on the corrupt policemen and their "victims," who keep trying to pay their way out of a violation - bogus or legitimate.

ix. Be ready to drive away when the policeman indicates that you may do so.

I. Use valet parking services at restaurants and hotels and make sure you get a legitimate receipt from the attendant before handing over the keys. **Also ensure your house or office keys are not on the key chain or ring you give to the attendant.** Remove all valuable items from the vehicle, including CDs, cassettes and loose change.

J. Avoid using side street parking if you do not know the neighborhood. The criminals are now coming to the better parts of town looking for cars to steal and victims to rob. If you are confronted by a carjacking situation and the criminal has a gun or knife in your face or at close proximity to your body, **do not resist**; turn the vehicle and its keys over immediately and wait for the criminals to drive away before you attempt to leave the area. Try to avoid going with them at all costs.

K. If you believe you are being followed by another vehicle, you may consider obviously using your mobile phone and looking back at the suspect vehicle to see if that will throw them off. Do not stop your vehicle for any reason until you are at a safe location, such as the hotel, office, shopping mall or restaurant and making sure that there are lots of other people around and in a well-lit area if at night. **However, if someone is in obvious pursuit, this would be the one exception to the rule about never looking to the police for assistance.** If being pursued aggressively, stop the first police patrol vehicle or policeman you see and report the incident. They might not do anything to detain the suspect vehicle, but the suspect vehicle will almost always break off the pursuit. You may then proceed to your original destination, but be on the lookout for the same suspicious vehicle or others and, if encountered, take similar evasive measures. Once safe at the hotel or office, report the incident to your company security officer immediately.

♦♦♦

Service of Process in Foreign Countries

By William F. Blake, CPP, CFE

The Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, more commonly called the Hague Service Convention,[1] is a multilateral treaty which was signed in The Hague on 15 November 1965 by members of the Hague Conference on Private International Law. It allows service of process of judicial documents from one signatory state to another without use of consular and diplomatic channels. The issue of international service had been previously addressed as part of the 1905 Civil Procedure Convention which was also signed in The Hague, which did not command wide support and was ratified by only 22 countries.

Diplomatic service via letters rogatory ...

Diplomatic channels are generally used between those states that are **not** contracting parties to the convention. It is generally affected by a *letter rogatory*, a formal request from the court in the country where proceedings were initiated or underway to a court in another country where the defendant resided. This procedure generally requires transmission of the document to be served from the originating court to the foreign ministry in the state of origin. The foreign ministry in the state of origin forwarded the request to the foreign ministry in the destination state. The foreign ministry then forwards the documents to the local court where the party to be served resided and the local court would arrange for service on the party to be served. Once service was made, a *certificate of service* (proving that service was made) would then pass through the same channels in reverse. Under a somewhat more streamlined procedure, courts can sometimes forward service requests to the foreign ministry or the foreign court directly, cutting out one or more steps in the process.

Procedure ...

The Hague Service Convention established a more simplified means for parties in signatory states to effect service in other contracting states. Under the convention, each contracting state is required to designate a "Central Authority" to accept incoming requests for service. A "Judicial Officer" who is competent to serve process in the state of origin is permitted to send request for service directly to the "Central Authority" of the state where service is to be made. Upon receiving the request, the Central Authority in the receiving state arranges for service in a manner permitted within the receiving state, typically through a local court to the defendant's residence. Once service is effected, the "Central Authority" sends a certificate of service to the 'Judicial Officer' who made the request. Parties are required to use three standardized forms: 1) a request for service, 2) a summary of the proceedings (similar to a summons), and 3) a certificate of service.

The Hague Service Convention established a more simplified means for parties in signatory states to effect service in other contracting states.

The main benefits of the Hague Service Convention over Letters Rogatory is that it is faster (requests generally take 2 - 4 months rather than 6 - 12 months), it uses standardized forms which should be recognized by authorities in signatory countries, and in most cases, it is cheaper because service can be effected by the local attorney without hiring a foreign attorney to advise on how to serve.

The Hague Service Convention does not prohibit a receiving state from permitting international service by other methods otherwise authorized by local law (for example, service directly by mail or personal service by a person otherwise authorized to service process in the foreign country). For example, in the United States, service can often be made by a private process server. States which permit parties to use these "alternative means" of service make a separate designation in the documents they file with the Convention.

Definition of court officers ...

In the United States, an attorney is regarded as an officer of the court, but not all countries accept them to "participate in their court procedures."

Continued on page 20 ...

ISPLA Report

by Bruce Hulme, CFE
Director of Government Affairs

As I write this article, Congress is in recess and not expected to return until after Labor Day; President Obama is evaluating options regarding possible retaliatory action to undertake in Syria; the Snowden affair regarding NSA's PRISM brings forth new revelations on a weekly - if not daily - basis; proposed legislation over information security breaches, amending the Electronic Privacy Communications Act, implementation of and/or cutting funding on the Affordable Care Act and proposed privacy legislation are stalled; and the proposed bills about which ISPLA has limited concerns have not been enacted, nor do we expect such to occur this year, if at all – except possibly 639/H.R. 1392, the Geolocational Privacy and Surveillance Act, a bipartisan bill that would outlaw GPS use without a court order. Still, we continue to monitor closely the actions of Congress and federal regulatory agencies. This report will concentrate on just seven topics that may be of general interest to some of INTELLENET's investigative and security professionals.

Federal Trade Commission Alleges Exposure of Medical and Other Sensitive Information Over Peer-to-Peer Network...

The FTC filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers.

The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

LabMD conducts laboratory tests on samples that physicians obtain from consumers and then provide to the company for testing. The company, which is based in Atlanta, performs medical testing for consumers around the country. The Commission's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data – including health information – it held. Among other things, the complaint alleges that the company:

- Did not implement or maintain a comprehensive data security program to protect this information;
- Did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information;
- Did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- Did not adequately train employees on basic security practices; and
- Did not use readily available measures to prevent and detect unauthorized access to personal information.

The complaint alleges that a LabMD spreadsheet containing insurance billing information was found on a P2P network. The spreadsheet contained sensitive personal information for more than 9,000 consumers, including names, Social Security numbers, dates of birth, health insurance provider information, and standardized medical treatment codes. Misuse of such information can lead to identity theft and medical identity theft, and can also harm

Continued ...

consumers by revealing private medical information.

P2P software is commonly used to share music, videos, and other materials with other users of compatible software. The software allows users to choose files to make available to others, but also createsva significant security risk that files with sensitive data will be inadvertently shared. Once a file has been made available on a P2P network and downloaded by another user, it can be shared by that user across the network even if the original source of the file is no longer connected.

"The unauthorized exposure of consumers' personal data puts them at risk," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users."

The complaint also alleges that in 2012 the Sacramento, California Police Department found LabMD documents in the possession of identity thieves. These documents contained personal information, including names, Social Security numbers, and in some instances, bank account information, of at least 500 consumers. The complaint alleges that a number of these Social Security numbers are being or have been used by more than one person with different names, which may be an indicator of identity theft.

The complaint includes a proposed order against LabMD that would prevent future violations of law by requiring the company to implement a comprehensive information security program, and have that program evaluated every two years by an independent, certified security professional for the next 20 years. The order would also require the company to provide notice to consumers whose information LabMD has reason to believe was or could have been accessible to unauthorized persons and to consumers' health insurance companies.

Because LabMD has, in the course of the Commission's investigation, broadly asserted that documents provided to the Commission contain confidential business information, the Commission is not publicly releasing its complaint until the process for resolving any claims of confidentiality is completed and items in the complaint deemed confidential, if any, are redacted.

NOTE: The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The issuance of the administrative complaint marks the beginning of a proceeding in which the allegations will be tried in a formal hearing before an administrative law judge.

"We envision that companies will have to have written procedures in place before a data breach. Failure to have such procedures will result in heavy fines and noncompliance will become a lucrative form of state revenue enhancement."

ISPLA has found that states have been instituting regulations and proposing legislation on protecting personally identifying information and confidential medical and financial data. We envision that companies will have to have written procedures in place before a data breach. Failure to have such procedures will result in heavy fines and noncompliance will become a lucrative form of state revenue enhancement.

ABA Resolution 118 on Cyber-intrusion ...

The American Bar Association at its annual meeting in August passed Resolution 118 pertaining to unauthorized and illegal cyber-intrusion of lawyers' computer networks. It is based on a 19-page report.

It should also be noted that Model Rule 1.1 provides that a lawyer shall provide "competent representation" to a client. This requires "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In summer 2012, the ABA comments to Rule 1.1 were amended to highlight the importance of technology to legal practice. Comment [8] to Rule 1.1 now states that a lawyer "should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology ..." The amendment does not impose new obligations on lawyers. Rather, it is intended to highlight the growing significance of technology to legal practice and emphasize a lawyer's responsibility to stay informed.

The duty is not necessarily for lawyers to become technological experts, but to ensure that they understand the impact of technology on the activities of a client or law firm. Technical proficiency implicates not only

Continued ...

adequate protection of confidential information, but providing adequate advice to clients on technological matters, including protection of the client's own data.

Professional investigators and security practitioners should also become familiar with the latest technology and protection of client data.

This report explains the American Bar Association's ("ABA") resolution regarding the growing problem of sophisticated intrusions into the computer networks utilized by lawyers and law firms. It notes the alarming rise of attacks on these electronic networks and the recent rise of nation states as significant actors in sophisticated hacking activities over the past decade. The report also condemns these unauthorized, illegal intrusions and urges governmental bodies at all levels—federal, state, local, territorial, and tribal—to examine, and if necessary, amend or supplement existing laws to deter and punish these intrusions but only in a manner that respects and protects client confidentiality, the broader confidential lawyer-client relationship, and traditional state court and bar regulation and oversight of lawyers and the legal profession. Further, the report notes the different measures available to combat sophisticated hacking, including diplomatic and law enforcement tools, legislation, and regulatory measures. This report also underscores the importance of protecting confidential client information, the attorney-client privilege, and other core legal principles. Finally, the report describes the ethical rules and professional obligations of lawyers and law firms implicated by information security breaches. This includes preventing unauthorized or accidental disclosure of client information and informing clients of such breaches should they occur. Overall, the resolution builds upon the several ABA resolutions passed by the House of Delegates and Board of Governors relating to information security and client confidentiality.

Increasing Cyber Attacks on Lawyers and Law Firms ...

As American businesses and government agencies become increasingly reliant upon network communications, they grow more vulnerable to information security attacks. Sophisticated attacks increasingly target critical infrastructure and national security assets as well as personal information. Criminals, terrorists, and nation states all see potential gains from attacking information systems. These threats to highly sensitive information trigger concerns from the national security community, privacy advocates, and industry leaders alike.

The Director of the National Security Agency estimates that the United States loses $250 billion each year due to cyber-espionage and other malicious attacks on information systems.

Confidentiality, integrity and availability are the three cornerstone goals that every data security program is designed to achieve. Malicious attacks exploiting security vulnerabilities take a number of forms. A common attack affecting "availability" and information access is a "distributed denial of service" ("DDoS") attack, whereby servers are overwhelmed when malicious attackers flood the bandwidth or other resources of the targeted system with external communications requests. Attacks on "integrity" cause improper modification of information by inserting, deleting or changing existing data. In an attack affecting "confidentiality," an eavesdropper can gain access to sensitive data whenever it leaves a secure area or is transmitted in an unsecure fashion (i.e., unencrypted).

Increasingly sophisticated methods are being developed for accessing confidential information. By using "phishing" or "spear phishing" attacks, intruders attempt to acquire information, such as login credentials. Masquerading as a trustworthy entity in an electronic communication, they entice users to open an e-mail attach-

Continued ...

attachment or click on a link to a website containing malicious software that will infect a network's computers and report sensitive information back to the intruders. These programs often remain undetected for months.

Attacks on confidential information on private networks can pose a direct threat to the economic and national security interests of the United States as well as the security of individuals and companies. Data collected by government agencies and by private information security experts over the past half-decade indicate a serious rise in state-sponsored hacking activities. "Attribution" techniques—which allow investigators to detect where cyber attacks originate—have improved, and information security experts have linked many recent sophisticated attacks on private organizations to state-sponsored actors. A 2013 National Intelligence Estimate identified state-sponsored hacking as a chief threat to the country's economic competitiveness. The report represents the consensus view of the United States intelligence community and describes a wide range of sectors that have been the focus of hacking over the past five years, including the financial, information technology, aerospace, and automotive sectors.

"... Mikulak comments that forensic psychologists and psychiatrists are ethically bound to be impartial when performing evaluations or providing expert opinions in court. However she has reviewed new research suggesting courtroom experts' evaluations may be influenced by whether they are retained by the defense or the prosecution."

As security experts in aggressively targeted sectors have ramped up security efforts, the information security firm Mandiant reports that sophisticated state-sponsored hackers have broadened their sights to include outside vendors and the business partners of high-value targets. Mandiant's comprehensive report on information security in the private sector points to an increase in sophisticated attacks on the networks of firms engaging in outsourced tasks, such as information technology, human resources, financial, and legal services.

Because law firms work with thousands of clients across numerous industry sectors, cyber intruders see law firms as lucrative storehouses of sensitive information. Companies seek counsel when they are engaged in deeply sensitive and highly expensive matters, which tend to generate information that is potentially of great value to third parties. Financial details concerning a merger or acquisition can give any interested outside entity an advantage in future negotiations. Similarly, lawyers have access to details about an organization's inner workings in the midst of litigation. Such information enables competitors to assess the financial stability of an organization and gain other tactical information. Furthermore, a firm's litigation strategy is often outlined in various intra-firm communications. These documents provide significant advantage to opposing parties or interested third parties when networks are successfully breached.

Law enforcement authorities in the United States, Canada, and the UK have all noted the rise in threats to law firm information systems. In November 2011, the Federal Bureau of Investigation convened 200 large law firms in New York City to urge them to review their cybersecurity policies. In 2012, the Director General of the British MI-5 informed the 300 largest companies in the UK that their information was as likely to be stolen from the computers of their attorneys and international consultants as from their own. The FBI does not track individual breaches or keep statistics on the types of businesses attacked, but a 2012 Mandiant report estimated that 80% of the 100 largest United States law firms were subject to successful data breaches by malicious intruders in 2011 alone.

Are forensic experts biased by the side that retained them?

A comprehensive study to answer this question was conducted by Daniel C. Murrie of the Institute of Law, Psychiatry, and Public Policy, University of Virginia and Marcus T. Boccaccini of the Department of Psychology and Philosophy, Sam Houston State University. They were assisted by Lucy A. Guarnera and Katrina A. Rufino. The research was funded by the National Science Foundation Law & Social Science Program.

In a recent article by Anne Mikulak, she comments that forensic psychologists and psychiatrists are ethically bound to be impartial when performing evaluations or providing expert opinions in court. However she has reviewed new research suggesting courtroom experts' evaluations may be influenced by whether they are retained by the defense or the prosecution. The research was published in *Psychological Science*, a journal of the Associa-

Continued ...

-tion for Psychological Science.

The findings reveal that experts who believed they were working for prosecutors tended to rate sexually violent offenders as being at greater risk of re-offending than did experts who thought they were working for the defense.

"We were surprised by how easy it was to find this 'allegiance effect,'" said psychological scientist Daniel Murrie of the University of Virginia. "The justice system relies often on expert witnesses, and most expert witnesses believe they perform their job objectively — these findings suggest this may not be the case."

He and co-author Marcus Boccaccini of Sam Houston State University have observed the adversarial justice system use forensic experts to gain an advantage in their cases. He stated "We became increasingly curious about whether forensic psychologists and psychiatrists could actually do what their ethical codes prescribed: handling each case objectively, regardless of what side retained them."

"...most people in this line of work really do try to be objective ..."

Murrie and Boccaccini decided to conduct a "real world" experiment, providing 118 experienced forensic psychiatrists and psychologists from several states the opportunity to participate In a 2-day workshop 108 forensic psychiatrists and psychologists utilized psychological tests to evaluate sexually violent predators. In exchange, the experts agreed to provide paid consultation to a state agency that was supposedly reviewing a large batch of sexually violent offender case files.

The experts returned weeks later to score risk assessment instruments for offenders (with attorneys) as part of the paid consultation – unbeknownst to them, each expert was given the same four files to review.

Even though the experts used the same well-known assessment instruments to evaluate the same offenders, the risk scores they assigned turned out to be significantly different depending on who they thought was paying them: Those who believed they were hired by the prosecution tended to assign higher risk scores, while those who believed they were hired by the defense assigned lower risk scores.

Murrie noted that most people in this line of work really do try to be objective, and not every forensic expert in the study demonstrated biased scoring. But the findings suggest that some of the experts were swayed by the side that retained them. "In short, even experts were vulnerable to the same biases as the rest of us, in ways that left them less objective than they thought."

The researchers hope that the study will prompt experts in this field to take a hard look at how evaluators are trained and how they practice. "Demonstrating that allegiance is a problem is the first step towards solving the problem," Murrie concludes. "The justice system certainly needs the expertise experts can offer, but the system also needs to be able to trust that their input is truly objective."

Strong Cooperation on Cross-Border Fraud...

The Federal Trade Commission signed a memorandum of understanding (MOU) with two Nigerian agencies on August 28 to increase cooperation and communication in their joint efforts to stamp out cross-border fraud. Nigeria's Ambassador to the United States, Adebowale Adefuye, provided opening remarks for the MOU signing ceremony.

The MOU was signed by FTC Chairwoman Edith Ramirez; Director General Dupe Atoki, of Nigeria's Consumer Protection Council (CPC); and Executive Chairman Ibrahim Lamorde, of Nigeria's Economic and Financial Crimes Commission (EFCC). It is the first FTC MOU of this kind to include a foreign criminal enforcement authority. The CPC addresses consumer complaints through investigations and enforcement; the EFCC is a criminal enforcement agency with authority to address consumer fraud and other financial crimes. More at: http://www.ftc.gov/os/2013/08/130828us-ncpc-efccmemo.pdf.

The EEOC Gets Slapped...

The U.S. District Court for the District of Maryland Bench denied the use of the EEOC's experts and ruled against the commission in a discrimination suit; and the

Continued ...

U.S. District Court for the Northern District of Iowa ordered the EEOC to pay $4.7M to defendant for costs and attorney's fees, believed to be the largest fee levied against the commission.

ISPLA recently commented on the two EEOC litigation cases brought against Dollar General and BMW regarding criminal record background checks conducted on minority job applicants and workers. Now we have two more to briefly report on. In the Maryland matter of EEOC v. Freeman, the Commission alleged that the defendant's use of credit and criminal histories violated Title VII. After dismantling and denying the use of the EEOC's experts, the Court ruled:

> *…even if [the expert testimony] were admissible, and summary judgment could not be granted for Defendant on that ground, the EEOC and their experts have still failed to identify the specific policy or policies causing the alleged disparate impact. Under Title VII, it is not enough for the plaintiff to show that "in general" the collective results of a hiring process cause disparate impact. Statistical analysis must isolate and identify the discrete element in the hiring process that produces the discriminatory outcome. Where a hiring process has multiple elements, the plaintiff must identify the element(s) that it is challenging and "demonstrate that each particular challenged employment practice causes a disparate impact," unless it can demonstrate that "the elements" are not capable of separation for purposes of analysis.*

The Court concluded its opinion:

> *The story of the present action has been that of a theory in search of facts to support it. But there are simply no facts here to support a theory of disparate impact resulting from any identified, specific practice of the Defendant. Indeed, any rational employer in the United States should pause to consider the implications of actions of this nature brought based upon such inadequate data. By bringing actions of this nature, the EEOC has placed many employers in the "Hobson's choice" of ignoring criminal history and credit background, thus exposing themselves to potential liability for criminal and fraudulent acts committed by employees, on the one hand, or incurring the wrath of the EEOC for having utilized information deemed fundamental by most employers. Something more, far more, than what is relied upon by the EEOC in this case must be utilized to justify a disparate impact claim based upon criminal history and credit checks. To require less, would be to condemn the use of common sense, and this is simply not what the discrimination laws of this country require.*

In August, the EEOC was ordered by the Northern District of Iowa to pay $4.7m in costs and attorney fees incurred by the prevailing defendant party in the case of EEOC v. CRST Van Expedited, Inc. Although this litigation did not concern credit or criminal history checks, its significance lies in the fact that the EEOC was ordered to pay costs and fees to the defendant, as a prevailing party. In a SeyfarthShaw blog this employment law firm posited that the Northern District of Iowa:

> *...held that the EEOC's conduct was in fact 'frivolous, unreasonable or groundless' given its blatant failure to exhaust Title VII's administrative prerequisites, including its failure to investigate and conciliate prior to bringing suit. Additionally, Judge Reade found that the EEOC's pattern-or-practice claim was unreasonable as it presented only anecdotal evidence in support of its claim and failed to present any expert evidence, statistics, or legal authority in support of its systemic claims.*

The blog adds that…

> *This is a significant if not stunning decision. It is believed to be the largest fee sanction award against the EEOC in its history.*
>
> *The ruling represents yet another powerful broadside to attack the EEOC's systemic litigation tactics and provides employers with more ammunition with which to challenge unreasonable and groundless claims by the EEOC. Particularly important for employers is the Court's rejection of the EEOC's argument that as long as it names one individual in a complaint and succeeds as to that individual, regard-*

Continued ...

-less of the frivolousness or unreasonableness of the remainder of its claim, an employer cannot be deemed a 'prevailing party' entitled to recover its fees.

District Judge Reade found the EEOC's conduct was in fact 'frivolous, unreasonable or groundless' given its blatant failure to exhaust Title VII's administrative prerequisites, including its failure to investigate and conciliate prior to bringing suit. Most likely the EEOC will appeal the decision.

The Fairness and Accuracy in Employment Background Checks Act of 2013 ...

This bill seeks to provide safeguards with respect to the Federal Bureau of Investigation (FBI) criminal background checks prepared for employment purposes. It calls for the Attorney General to establish and enforce procedures to ensure the prompt release of accurate records and information exchanged for employment-related purposes through the records system created under section 534 of title 28, United States Code. This same bill has been offered by Representative Robert C. Scott (D-VA3) in the past several Congresses. It has failed each time and we expect it will not pass in the 113th Congress as well. In 2010 ISPLA met with Congressman Scott regarding indigent defense issues, as well as this bill.

The accuracy of FBI background checks for employment purposes has come under greater scrutiny recently. The National Employment Law Project (NELP) released a report in July 2013 titled "Wanted: Accurate FBI Background Checks for Employment" that found as many as 600,000 of the nearly 17 million employment background checks the FBI processed in 2012 contained inaccurate information. The NELP report is available at: http://nelp.3cdn.net/bd23dee1b42cff073c_8im6va8d2.pdf.

♦♦♦

Bruce Hulme, CFE, is ISPLA's Director of Government Affairs (www.ispla.org). ISPLA is a resource for the investigative and security professions, U.S. and state governments and the media.

Service of Process in Foreign Countries

Continued from page 13…

Service by mail ...

The interpretation of a provision in article 10(a) is controversial. The provision permits the requesting judicial officer to "send" judicial documents by postal channels to countries that authorize this usage in ratifying the convention, such as France and Italy. Other provisions of the convention say "serve" or "service." The controversy is over whether the provision permits service directly on parties by mail. In the United States, some courts interpret this provision to permit service by mailing documents directly to individuals; others hold that the provision only authorizes sending, but not serving, documents by mail. The European Court of Justice and courts in Greece and Alberta interpret the provision to permit formal service by mail. Other countries, including Germany, Switzerland, and most current and former communist countries, require incoming service to be effected exclusively through the country's central authority

Relation with other instrument ...

Under the convention, countries may conclude different agreements between them that take precedence over the convention. Thus, within the European Union (except for Denmark) Council Regulation (EC) No. 1348/2000 applies instead of the convention.

♦♦♦

Bill Blake is owner of Blake and Associates, Inc., Littleton, Colorado.

Footnote: (1) For participating countries, see Wikipedia, *Hague Service Conventions*, http.//en.wikipedia.org,wiki/hague_service_convention. Text is available under the Creative Commons Attribution-Share Alike License.