INTELLENET *News*

Official Newsletter of the International Intelligence Network, Ltd.

Intellenetwork.org *Summer 2018*

In this issue ...

Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet

Dear Intellenet Members: We have a lot going on these days …

I hope everyone is having a great summer and business is going well. Intellenet has a lot going on these days. We are currently working with a web development company to create a new dynamic website for the association. This new website will have a lot of key items on it that are sure to help not only members, but those looking to hire our members. As you have seen on the listserv, our 2019 conference location and dates have been announced. The conference will take place at the Marriott City Center Hotel located in Charlotte, NC. The dates of the conference are April 2-5, 2019. Make your reservations here.

Our education director, Jeff Stein, has been putting together another great speaker line up for the conference. Our conference local hosts, Don and Gina Hubbard are also working on fun events for everyone. This is sure to be another great conference event.

Our assistant executive director Ed Spicer is hosting a seminar sponsored by Intellenet in Massachusetts this September 15, 2018. The location is at the Cummings Center in Beverly, MA. For more information on this one-day seminar contact Ed Spicer at ed@oceanstatesinv.com.

Intellenet will continue to attend investigation and security conferences. Of particular note this year is the International Protection Security Board-Close Protection conference being held in Las Vegas, NV on November 29-December 4, 2018. For the last several years this conference has been attended by over 300 protection professionals. We have been asked to be a vendor there to provide investigative resources that are needed by those attending. We also will continue to attend state and regional conferences in support of those efforts as well as potential recruitment of new members.

The BAI program was kicked off at our Las Vegas conference in 2015. While the program got off to a little bit of a rocky start, it has progressed into a streamlined professional modern program. All applications, testing, and CEU updates are done online with the exception of the in-person peer review. For more information about this program go to the BAI website located at http://www.baipi.org/.

It is that time of the year to update the Intellenet Speakers Bureau information. The Speakers Bureau program is a valuable branding and marketing program for Intellenet and you as a professional investigator, security consultant or support services provider. If you have not seen this document, you can find it on the home page of the Intellenet website. For those of you ever looking for a speaker at your state association conferences or for a client, this is a great resource. If you would like to update your listing or be included, Please contact Bill Blake at billblake2@aol.com.

As always you can reach me at peter@ewiassociates.com.

♦♦♦

Member News

Welcome New Members ...

Wesley CLARK — Southington, CT

(Wesley's a longtime supplemental support member, now a licensed PI.)

Michael GIBBONS — Western IRELAND

Tom JAEB — Minneapolis, MN

(Tom replaces Paul Jaeb.)

Martin JAEKEL — Toronto, CANADA

Tony OLIVO — Buffalo, NY

Adley SHEPHERD — Tacoma, WA

Tawni TYNDALL — Granada Hills, CA

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.

September events ...

On the 15th ***Intellenet*** is hosting the fall seminar of the North-East Professional Investigators Network at the Cummins Center in Beverly, Massachusetts.

Intellenet members are featured speakers, including attorney **Dennis Crowley** speaking on "The Power of Indemnification in Your Investigative/Security Contract." Ed notes that *"Dennis is particularly skilled in scaling business operations, developing client relations, strategic planning, sales & marketing, human resources, quality control, security operations, & corporate law."*

Thomas Howard is the proprietor of Howard Consulting & Investigative Group, which he founded in 2008. He utilizes his past training and experience in the areas of risk management and workplace violence to assist clients in solving those issues that can be harmful to the overall operation of their businesses. Howard has over 30 years in law enforcement and holds a Master's in Criminal Justice from Anna Maria College.

Intellenet member **Robert Wile** will speak on "Sexual Assault Investigations: The *do's & don't's* of interviewing suspects, victims & witnesses." Robert worked at the Amesbury Police Department as a detective of the Domestic Violence & Sexual Assault Unit from 1998-2017. His assignments also included the investigation of child and elder abuse cases. Robert holds a MEd in Counseling/ Psychology from Cambridge College.

Intellenet Assistant Executive Director **Ed Spicer** sent this note about a featured speaker on detecting fraudulent identifications:

*"Caroline Guarino is a Senior Special Investigator with the Commonwealth of Massachusetts Alcoholic Beverages Control Commission for 2*Assistant Executive Director **Ed Spicer** *3 years. Aside from her investigator duties, Caroline teaches classes on the laws of the Liquor Control Act at police academies across the state and trains license holders and local licensing boards on liquor law, procedures and regulations. As a police officer with the town of Topsfield, Caroline was the department DARE officer, Sexual Assault Officer and RAD Kids Instructor. Caroline worked as an undercover narcotics officer for five years on the North Shore."*

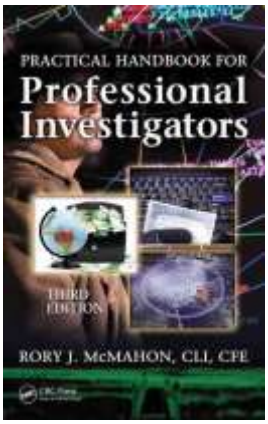
All proceeds from the seminar benefit Intellenet Scholarship Fund. To register contact Ed at ed@oceanstatesinv.com.

On the 18th **Bruce Sackman**, President of the Society of Professional Investigator, releases a new book, "Behind the Murder Curtain: Special Agent Bruce Sackman hunts doctors and nurses who kill our veterans."

On the 20th Bruce's book will be available during the Society of Professional Investigator's annual dinner in New York City. For details, go to https://spionline.info/.

Member News continues on next page ...

Also in September, Intellenet member **Rory J. McMahon**, Ft. Lauderdale, FL, partners with Bergen Community College in Paramus, NJ to offer a Certificate in Professional Investigation Program. The course will run for 100+ hours and include 11 modules which cover the gamut of professional investigative courses.



Rory's book, Practical Handbook for Professional Investigators, 3rd edition, will serve as the primary textbook. Any members in the NJ area interested in teaching some of the modules please contact Rory directly at rory@mcmahonpi.com.

Coming in October …

Brandy Lord, president of the Indiana Society of Professional Investigators, is excited to announce they are hosting Brandon Perron, CCDI, CFI-FTER, with the Criminal Defense Investigations Training Council, for a two-day course covering forensic interviewing and certification in the forensic testimonial evidence recovery method. The training will be hosted on October 26-27, 2018 at the Double Tree Hotel in South Bend, IN. If you are interested in attending, visit the INspi website at www.indianainvestigators.com for additional details and registration. For questions relating to training, contact 574-288-5911.

And in November …

Kevin McClain, CCDI, BAI will be presenting "Investigating Sex Assault Cases on Every Budget" at NACDL's 9th Annual Defending Sex Cases Seminar. Kevin's talk is part of the seminar's program titled "Defending the Unthinkable: Zealous Advocacy in Sexual Assault and Child Victim Cases." The seminar is at the Planet Hollywood Hotel in Las Vegas, NV on November 16-18, 2018.

In other news …

Intellenet members **David Shelton,** left, of Vincennes, Indiana and **Ken Shelton**, Angola, Indiana recently attended an event in Indianapolis featuring Indiana's Lt. Governor, Suzanne Crouch, seen here. David and Ken are local elected officials in their respective communities. No, they're not related.

The International Association of Security and Investigative Regulators invites you to their 25th Anniversary in Scottsdale, Arizona, October 24-26, 2018, at the beautiful Saguaro Scottsdale Resort. Licensing regulators and industry members from several states and provinces will be in attendance. Intellenet members **Bruce Hulme, CFE** and **Don C. Johnson, CLI** serve on IASIR's board of directors. For details on the conference, go to www.IASIR.org.

♦♦♦

CASE STUDY

Beyond Social Media: Manual Image Matching Techniques

By Brad Trew
Director, Cyber/Special Investigations, Reed Research

Social media can give an investigator a wealth of information to work with. In some instances, additional information is required to further the case when conventional search methods do not work.

There are various tools such as Google Image Search, TinEye and others that will do online image searches, but these will typically just find other locations hosting the same image.

This article will explore how to examine beyond the surface information by analyzing various available clues in a photograph to gather additional intelligence. We have had great success in locating subjects, assets, addresses and missing persons using these methods.

These searches can be very labour intensive and are mostly the result of trial and error, tenacity and fortuitous luck. The reward is that you can develop information and results that traditional methods cannot.

Case Example 1:

In a recent example, we were asked to develop information about the activities and movements of a Canadian citizen. Through traditional social media search techniques, we developed the photo of him below.

From the photo below, **Case Example 1, Photo 1**, it could be ascertained that the subject is seated in what appears to be an amusement park ride and looks like he has water behind him. As the photo was posted in April, it was believed that he was in a locale that was warmer than the

Continued ...

Case Example 1, Photo 1

Canadian climate at the time. Using Google's image search, we searched different terms related to "amusement," "ride" and "water" and compared images looking for similar high back black seats with three openings and a metal bar, and rock walls. Numerous results were found then discarded as we refined our search methods several times to narrow down our findings. The searches found a picture that identified a water-based amusement park ride with similar looking seats. The location was determined to be "Grizzly River Rapids" at Disney's California Adventure theme park in Anaheim, CA.

The first image below, CASE EXAMPLE 1, PHOTO 2, shows similar high back black seats with three openings and a metal bar. Although the ride is water-based, the environs did not match the subject photo.

Further searches regarding Grizzly River Run Rapids found a video of the ride which shows a point-of-view perspective of the ride from start of finish., seen below in CASE EXAMPLE 1, PHOTO 3 The same rock wall, as shown behind the subject, can be seen at the 5:54 mark.

Continued ...

CASE EXAMPLE 1, PHOTO 2
SOURCE: GETTY IMAGES

CASE EXAMPLE 1, PHOTO 3
SOURCE: YOUTUBE

Case Example 1
Photo 4 — Photo 5

By comparing the questioned image with a video still from the above video, seen in the examples in Photos 4 and 5, we can see that both were taken in the same location. As an added bonus, the person is a Canadian national who, based on these findings, had travelled to the United States. In consideration of U.S. Customs restrictions, we can make the assumption that this person does not have a criminal history and is free to travel outside of Canada.

Case Example 2:

A similar technique was also applied in locating a subject. We were provided with a questioned photo that showed a photo taken from an elevated position looking between two apartment buildings. Because of foggy weather, there were no other points of reference.

From this photo, we could conclude certain facts:

✦ The photo was taken from an elevated level of approximately 100' or more.

✦ The location was part of an apartment complex comprised of at least three high-rise apartment buildings; the building where the photo was taken and two other buildings shown in the photo, one taller than the other.

✦ The buildings appeared to be an older style common in the Toronto area and not the type presently being built in and around the downtown core.

The buildings had unique characteristics. For instance, we noted that the building on the left side of the questioned photo had a single line of windows down the right side of the building whereas the building on the right had black balconies.

Through developing our subject's social media further, we were able to locate a Twitter profile. In reviewing the

Case Example 2, Photo 1

Twitter feed, we located another photo taken from the same perspective eight month's previous. The photo was taken at night, seen here (CASE EXAMPLE 2, PHOTO 1); however, the same two apartment buildings can be seen in the same relative positions and the CN Tower, located in downtown Toronto, can be seen illuminated in the distance.

CASE EXAMPLE 2, PHOTO 2

We compared the questioned photo (below left) with the developed photo of the CN Tower that was located (below right). Both apartment buildings appear in both photos which confirms they were taken from the same location. It was also concluded that the photos were taken from a considerable distance away from the CN Tower.

Google Image Search was used to locate daytime images of the CN Tower to determine the perspective of the questioned photo in relation to downtown Toronto. It was noted that there are no tall buildings in close proximity the CN Tower which would suggest that it was taken from either the northeast or northwest. Also noted was that downtown appears to the left of the CN Tower which would suggest the photo was taken from the west.

"These searches can be very labour intensive and are mostly the result of trial and error, tenacity and fortuitous luck. The reward is that you can develop information and results that traditional methods cannot."

Google Earth satellite images were utilized to search for high-rise apartment complexes west of the downtown core. This process was a lengthy trial and error process as there were no clear indicator as to where the complex was located. In all, approximately three dozen neighbourhoods were searches and examined.

Continued ...

This search located the apartment complex in question.

From a database of high-rise apartment buildings, it was established that the building on the left side of the photo is a 12-storey building. In the questioned photo above, it can be seen that the roof of the building is not visible, and it does not appear that the photographer is looking upwards. From this, it could be determined the floor from which the photo was most likely taken. A physical attendance was then made to the vicinity of the high-rise apartment complex, to narrow down our search.

Utilizing the questioned photograph, we analyzed the perspective of the balconies of the building to the left side of

the photo and positioned myself to match the same perspective on the ground.

Based on the searches done, we were able to determine which building, floor and unit number the subject resided in.

My next article will explore geo-location based searches using various social media platforms.

About Brad Trew:

Brad Trew is the Director of the Special Investigations/ Cyber Unit at Reed Research Ltd. in Toronto, Canada. Brad specializes in high-level investigations throughout the fraud realm by managing the questionable aspects of technically challenging claims throughout North America, and Internationally. Brad's expertise impacts a large menu of cases from death claims to missing persons, and Regularly includes background profiles, arsons, witness statements, corporate issues, and other complex matters through the use of deep web, OSINT and HUMINT investigation strategies. Brad has extensive experience with investigations leveraging technology such as cyber threat analysis, computer forensics, cargo security, loss prevention, business continuity planning, kinesic interviewing, asset and target tracking while employing GPS, cellular and RF technology, and leveraging his technical counter-surveillance measures and covert video applications experience. Should you wish to discuss a matter with Brad or draw on his knowledge, he can be reached at Brad.Trew@ReedResearch.com.

♦♦♦

SKIPTRACING

By Óscar Rosa

Nowadays, skiptracing reports are basic to anyone in need of information about private individuals and companies. Private investigators play a main role against the usual channels of commercial information by providing worthy, legal and accurate material, crucial for any company interests.

INTRODUCTION

In the twenty-first century, skiptracing is a service demanded to private investigators worldwide. Financial institutions, insurance companies, law firms, collection agencies, legal departments in private entities and other collaborative detectives, trust the information provided by these professionals regarding contact details such as the address or the telephone number of a private individual or a company, subject to an investigation.

Two reasons apply to the request of this sort of assignments. On the one hand, the first reason why a skiptracing report is requested to a private investigator is to find out information which is different to the one provided by the usual channels. The client profile in the twenty-first century is different from the ones in previous periods. Nowadays, they have become amateur investigators who make previous arrangements to gather information regarding the subject. It is then, when the client has already tried to locate the subject at their own means and the search has proved unsuccessful, that the services of the private investigator are required.

Continued ...

On the other hand, the skiptracing report of a private investigator is required because of the worthy legal aspects regarding the data provided. A particular address delivered by a private investigator is legally guaranteed. Regarding Spain, this legal guarantee contributes to the absence of reputational risk for a company, since the private investigator profession is regulated by Law and their reports are acknowledged by Justice.

The twenty-first century private investigator contributes with their investigations to provide skiptracing reports which include legal and divergent information, such as a particular address and a verified contact telephone number. This sort of data cannot be provided by any other provider of commercial information.

Nevertheless, this type of investigation is not a novelty, since the first acquainted skiptracing requests on individuals or companies date from the mid-nineteenth century, as can be seen in several advertising examples, the earliest of them dated 1860.

The routines to follow and the sources of access in a skiptracing investigation are different whether a private individual or a company is involved.

Private Individuals

The information regarding private individuals is regulated by the laws of data protection. Consequently, the access to this sort of information is restricted.

The regulation on data protection is different according to the country. In the European Union, especially in Spain, the source of the collection of data such as particular addresses or telephone numbers is regulated under strict laws and strong punitive actions by the Spanish Agency of Data Protection (AEPD). Therefore, the information has to be obtained from a public source or with the full consent of the inquired individual, provided, for instance, during the course of an interview.

According to the previous information, the importance of a report signed by a Spanish private investigator remains in the fact that it becomes

a private source of valuable data which can be used for the benefit of the client as it has the exclusive possibility to include personal data which cannot be achieved by others.

However, there is an essential condition to be fulfilled in order to request a skiptracing investigation: the client needs to advance a legitimate interest, in other words, to provide arguments that support the grounds on which the skiptracing report is requested. For instance, a financial entity can request an assignment to locate the address of a debtor who cannot be located.

In Spain, the private investigator profession is regulated by Law since April 2014. The article 48.1 in the Law of Private Security sets out that:

"The services regarding private investigation, provided by private investigators, will consist in the carrying out of inquiries which are necessary to obtain and provide, on behalf of a third legitimate part, information and evidence of behaviour or private facts related to the following aspects:

> *The economic, labour, commercial, financial ambits, as well as private, familiar or social lives, excluding those developed in private homes and reserved places."*

Telephone Numbers

The telephone number is one of the most used means of contact, for instance, by collection agencies which most usually possess outdated information about the debtor and need different and updated telephone numbers. In cases like this, the target of the private investigator is to locate the number by means of their own experience and professional skills, by contacting relatives, neighbours, friends or other sources close to the private individual.

Two types of telephone numbers might be found throughout the process of investigation:

- *A landline telephone number which is associated with a home address or a business.* This sort of telephone number has one disadvantage: there has to be someone to answer the call whenever it is made. In other words, the call might be made when nobody is at home or, if it is a business address, the call might be unsuccessful because of the schedule hours. Once the telephone number is

located, it is important to develop an Internet research, since the results obtained may lead to a new line of investigation.

- *A telephone number which is directly linked to a specific individual.* This sort of telephone number holds an extra value and increases the possibilities of contact. Instant messaging applications like Whatsapp or Telegram, may allow to verify and re-enact the behaviour of the individual, as well as to provide a profile of the ideal contact schedule.

Address

The address is a type of information required for some purposes of communication, such as handing a judicial notice or a court injunction.

This information is usually provided by the client when the assignment is made. However, this information is likely to be partial and outdated. It is the task of the private investigator to, by means of their skills, complete the missing data or locate a different accurate address.

The fields needed to complete an address are four: name of the street, along with the number of the location, postal code, town/city and province.

There are two types of address:

1) *Home address:* It is the private address of the debtor, which must be verified by the detective. The sources of investigation regarding this type of address are several, being the neighbours of the individual a frequent source of information. The depth and detail of the home address investigation and the description provided depends on the client needs. For instance, sometimes it is important to perform an examination of the area where the address is located, ascertain whether it is a property of the debtor or they live there as tenants, or carry out an inspection of the grounds.
2) *Business address:* It is the location where the individual investigated develops their professional activity. This address might correlate to a business centre, an office, a shop, a commercial premise, etc.

Information required to launch an investigation after a private individual

- *Name:* In Spain, people have two family names. The first one corresponds to the first surname of the father and the second one matches the first surname of the mother. The combination of the family names, together with the first name, may turn out a unique outcome, i.e. only one person has a determined sequence of name and surnames; or it may be a common name, in which case several individuals have the same combination of first name and family names.
- *Identification document number:* In order to avoid misunderstandings and increase efficiency, the client must provide the national identification document number, the residence document number or the passport number along with the rest of the information provided before the skiptracing enquiry.
- *Date and place of birth:* These are some of the most important facts to carry out a skiptracing investigation, since they may help to dismiss people who have similar names in a social network, as well as the birth place may serve as a clue and starting point.
- *Home address:* As with the information above, it is a starting point for the skiptracing investigation. Even if the home address provided by the client may be incomplete, it does help in the course of the investigation.

Sources of access to the information of a private individual

The sources of access to this type of information differ whether the investigation is carried out after a private individual or a company.

- *Land Registry:* In Spain, it is a global registry that gathers data about all the records of every town or city. The name of a person or their identification number must be provided in order to perform a search in the archive, the result of which may lead to an address which is directly linked to the individual investigated or a business related to them.
- *Commercial Registry:* It is a registry common to the vast majority of countries in the world. In Spain, a centralised registry is available, which includes every company and company administrator, despite the town or city of provenance. By providing accurate facts about an individual, such as their name and identification number,

the registry delivers information about the companies related to them.

- *Internet:* A search by name provides restricted information when it comes to a web investigation, since the name by itself may not be sufficient if further information, such as the identification number of the individual, is lacking. Quite a lot of information will have to be dismissed if we are uncertain about the identity of an individual in a social network, forum or official publication. However, if the search is performed under the national identification number, there is a guarantee that the results found in the Internet are associated to the person we are trying to investigate. On the contrary, the information about a company available in the web is far more intensive than that of an individual, since corporate and advertising details, websites, and many other facts are usually available.
- *Social networks:* Social networks may provide valuable information about the location of an individual inquired about. A picture, a shared location, the friends with whom they share comments or feedback, may help to dismiss or verify specific information.
- *Chambers of Commerce:* Although not every professional is registered in the chambers of commerce, they provide information about freelancer individuals sorted by their professional activities. The chambers of commerce are one of the few sources of information allowed by the Spanish Agency of Data Protection.
- *Business reports:* They provide structured information about companies and their administrators which is recorded in the Commercial Registry.
- *Telephone number data bases:* They are basic tools regarding the research of telephone numbers linked to specific addresses. These data bases are useful as well to locate relatives, neighbours and businesses related to private individuals.
- *Geolocation tools:* More and more companies offer geolocation tools which analyse mobile telephones or pictures published in social networks.
- *Email addresses:* The email address as a means of contact is also a usual request by the clients, as it is usually linked to a smartphone. It is important to verify the legitimacy of the email address. Some Internet companies provide a free service of email verification.

Companies

The information regarding companies is subject to fewer legal constraints than the one regarding private individuals. In most cases, the private investigator might find out some information useful as a starting point, although it is also common that the company subject of investigation remains closed or inactive, in which case the address of an associated operating company must be located. If the company relates to a small business, the detective needs to locate the address of the administrator.

It is advisable to include the name of the street as well as further details in an Internet search engine. The results obtained may provide us with a better knowledge of the nature of the address we have found and it will lead us to every website where the address is included, unveiling associated companies; changes regarding the brand name or if the address retrieved relates to a business centre.

During the course of the investigation, tools like Google Maps are likely to be used, since they virtually locate the address we are looking for. These tools may help us to anticipate an onsite visit as well as to find potential companies and nearby business.

Telephone number

The telephone number of a company office is usually a landline attended by an operator according to a defined schedule which must be considered. A skilled private investigator can verify the accuracy of a telephone number.

It is important, once a company telephone number is located, to test it in every Internet search engine available, since the results may provide information of interest, such as linked companies which use the same number.

Address

Four requirements are needed for an address to be considered as accurate:

1) Name of the street, including the number of the location
2) Postal code
3) City or town
4) Province

A distinction must be made according to the address of a company. On the one hand, there is a social address, that is, the official address of the company. On the other hand, there is an operation address, in other words, the place where the activity of the company is carried out. In some cases the social address and the operation address may be the same.

Data required to launch an investigation after a company

- *Name of the company:* When it comes to launching an investigation, it is essential to arrange the accurate and full name of the company, since it helps us to earn some time and prevents us from wasting money in flawed research involving official agencies. Once the assignment of an investigation is made, the clients usually provide commercial brand names or anagrams which may slow down the launching of the investigation. In cases like these, a previous work of investigation must be made in order to find out the right data behind them.
- *VAT number:* This fact may be the key to launching an investigation and to provide certainty that the company being investigated is the right one.
- *Address:* Even though the information which the client provides might be useless for the private investigator, it could still act as a clue to find out a new accurate address.
- *Operations:* Previous knowledge provided by the client about the purposes of a company investigated may help the private investigator to dismiss companies which have similar names.

Sources of access to the information of a company

- *Official agencies:* As with private individuals, it is possible to carry out an investigation in a variety of registry offices, such as the property or mercantile registries, which may provide information about the addresses belonging to the company or the place where it is operative.
- *Website:* The website of a company is one of the first steps to be checked during the course of a skiptracing investigation. The page providing information about the means of contact or the location of the company may provide an address that should be verified in a second step.
- *Credit Report:* Credit reports ought to be one of the first enquiries in the investigation. Some companies provide rough mercantile information worldwide as well as some are specialised in a certain country. Consequently, it might be very easy to find the ideal provider.
- *Internet Data:* Valuable quality information can be found by means of the search engines at our disposal, which may give us guidance on the accuracy of the address. Every company is a different world, according to that, the results obtained can be diverse.

Conclusions

In short, skyptracing is crucial to a great variety of clients worldwide. The investigation of a private investigator starts where the public sources of information, open to the companies, end. As a private source of information, skiptracing reports made by private investigators provide worthy material and legal guarantees.

Process and management of the investigation vary whether the enquiry regards a private individual or a company, as well as the sources of information are different when it comes to a company or a private individual, being more restricted to the latest.

The greatest amount of information provided by the client, the more opportunities for success arise for the private investigator in a skiptracing report. Therefore, it is our duty to persuade the clients to provide enough information in order to launch an efficient skiptracing investigation.

♦♦♦

Óscar Rosa is with the Contrasta2 agency in Malaga, Spain. He can be reached at Oscar@contrasta2.es. They specialize in compliance with the FCPA / AML, skiptracing and surveillance.

ISPLA News for INTELLENET

By

Bruce Hulme H. Hulme, CFE, BAI

ISPLA Director of Government Affairs

As the director of government affairs for Investigative and Security Professionals for Legislative Action (ISPLA) and legislative liaison board member of INTELLENET concerned with legislative and regulatory issues, I have often given presentations or written about potential pitfalls affecting private sector investigations. Recent hot topics have included License Plate Readers and the use of Drones and GPS tracking to conduct surveillance. Longstanding issues have included the avoidance of Gramm-Leach-Bliley Act (GBLA) violations while locating assets or recovering ill-gotten gains and stolen property, compliance with the Fair Credit Reporting Act (FCRA) when conducting pre-employment and third-party workplace investigations, avoiding potential invasion-of-privacy lawsuits when conducting surreptitious surveillance or open-source intelligence and social media investigations, and the use of pretense, a recognized investigative tool when conducting interviews of witnesses and targets of investigations. All of the foregoing topics have been part of legislative or regulatory oversight of private sector professional investigators that have I have addressed before members of Congress for ISPLA since its inception in 2009, and prior to that for NCISS and ALDONYS. Many of the regulatory and legislative issues that have confronted the professional investigator and security professional have arisen from privacy issues.

Many of these issues have also been discussed by me at numerous annual seminars of the International Association of Security and Investigative Regulators which will hold its 25th Annual Conference in Scottsdale, AZ from October 24-26. Leadership from throughout IASIR's 25-year history will reflect on changes in the regulated industries of private investigation, contract security, armored cars and alarm systems, ways that licensure has evolved, and the role IASIR has played in encouraging professionalism through effective regulation. Current and anticipated challenges will also be addressed. I hope that our INTELLENET members will consider attending this event. Details are at www.IASIR.org.

"At the 25th annual conference of the International Association of Security and Investigative Regulators this October, I will reflect on changes in our regulated industries and the ways that licensure has evolved, and the role IASIR has played in encouraging professionalism through effective regulation. Please consider attending. Details at www.IASIR.org. "

Facial Recognition Technology: The need for public regulation and corporate responsibility

Facial recognition technology has advanced rapidly the past decade. "Tagging" a face on Facebook or another social media platform with a suggested name is facial recognition at work. Tech companies utilizing this technology have turned time-consuming work to catalog photos into something both instantaneous and useful.

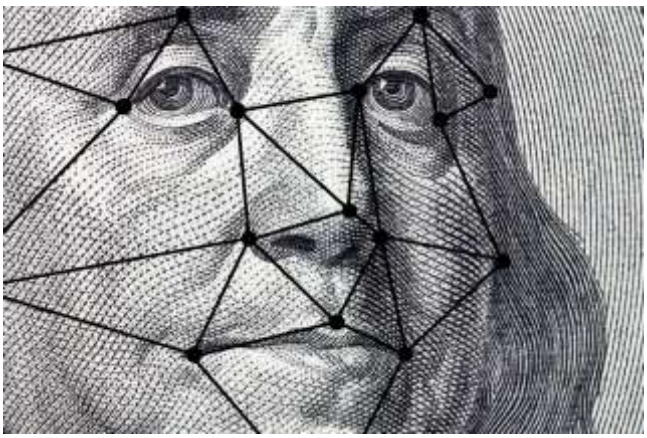
The ability of computer vision to get better and faster in

recognizing people's faces reflects better cameras, sensors and machine learning capabilities. The advent of increasingly larger datasets as more images of people are stored online and the ability to use the cloud to connect all this data and facial recognition technology with live cameras allows the captured images of people's faces and seeks to identify them – in more places and in real time.

"Advanced technology no longer stands apart from society; it is becoming deeply infused in our personal and professional lives. This means the potential uses of facial recognition are myriad. At an elementary level, you might use it to catalog and search your photos, but that's just the beginning. Some uses are already improving security for computer users, like recognizing your face instead of requiring a password to access many Windows laptops or iPhones, and in the future a device like an automated teller machine," according to Smith who pointed out additional uses as follows:

"Some emerging uses are both positive and potentially even profound. Imagine finding a young missing child by recognizing her as she is being walked down the street. Imagine helping the police to identify a terrorist bent on destruction as he walks into the arena where you're attending a sporting event. Imagine a smartphone camera and app that tells a person who is blind the name of the individual who has just walked into a room to join a meeting.

"But other potential applications are more sobering. Imagine a government tracking everywhere you walked over the past month without your permission or knowledge. Imagine a database of everyone who attended a political rally that constitutes the very essence of free speech. Imagine the stores of a shopping mall using facial



recognition to share information with each other about each shelf that you browse and product you buy, without asking you first. This has long been the stuff of science fiction and popular movies – like "Minority Report," "Enemy of the State" and even "1984" – but now it's on the verge of becoming possible.

"Perhaps as much as any advance, facial recognition raises a critical question: what role do we want this type of technology to play in everyday society?"

Facial recognition is advancing quickly but remains far from perfect. Biases have been found in the performance of several fielded face recognition technologies. The technologies worked more accurately for white men than for white women and were more accurate in identifying persons with lighter complexions than people of color. Even if biases are addressed and facial recognition systems operate in a manner deemed fair for all people, there will still be potential failures. "Facial recognition, like many AI technologies, typically have some rate of error even when they operate in an unbiased way. And the issues relating to facial recognition go well beyond questions of bias themselves, raising critical questions about our fundamental freedoms," wrote Smith.

Politics Meets Silicon Valley

As the country was transfixed by the controversy surrounding the separation of immigrant children from their families at the southern border, a tweet about a marketing blog Microsoft published in January quickly blew up on social media and sparked vigorous debate. The blog had discussed a contract with the U.S. Immigration and Customs Enforcement, or ICE, and said that Microsoft had passed a high security threshold; it included a sentence about the potential for ICE to use facial recognition.

Microsoft since confirmed that the contract in question isn't being used for facial recognition at all. Nor has Microsoft worked with the U.S. government on any projects related to separating children from their families at the border, a practice to which they have strongly objected. The work under the contract instead was "supporting legacy email, calendar, messaging and document management workloads**."**

Broader questions that are rippling

across the tech sector are not unique to Microsoft. They surfaced earlier this year at Google and other tech companies. Amazon employees objected to its contract with ICE, while reiterating concerns raised by the American Civil Liberties Union (ACLU) about law enforcement use of facial recognition technology. Salesforce employees have raised the same issues related to immigration authorities and these agencies' use of their products. Demands increasingly are surfacing for tech companies to limit the way government agencies use facial recognition and other technology. These issues are not going to go away. They reflect the rapidly expanding capabilities of new technologies that increasingly will define the decade ahead. Facial recognition is the technology of the moment, but it's apparent that other new technologies will raise similar issues in the future. This makes it even more important that we use this moment to get the direction right.

The need for government regulation

The only effective way to manage the use of technology by a government is for the government proactively to manage this use itself. And if there are concerns about how a technology will be deployed more broadly across society, the only way to regulate this broad use is for the government to do so. This in fact is what we believe is needed today – a government initiative to regulate the proper use of facial recognition technology, informed first by a bipartisan and expert commission.

While we appreciate that some people today are calling for tech companies to make these decisions – and we recognize a clear need for our own exercise of responsibility, as discussed further below – we believe this is an inadequate substitute for decision making by the public and its representatives in a democratic republic. We live in a nation of laws, and the government needs to play an important role in regulating facial recognition technology. As a general principle, it seems more sensible to ask an elected government to regulate companies than to ask unelected companies to regulate such a government.

> **"As a general principle, it seems more sensible to ask an elected government to regulate companies than to ask unelected companies to regulate such a government."**

Such an approach is also likely to be far more effective in meeting public goals. After all, even if one or several tech companies alter their practices, problems will remain if others do not. The competitive dynamics between American tech companies – let alone between companies from different countries – will likely enable governments to keep purchasing and using new technology in ways the public may find unacceptable in the absence of a common regulatory framework.

It may seem unusual for a company to ask for government regulation of its products, but there are many markets where thoughtful regulation contributes to a healthier dynamic for consumers and producers alike. The auto industry spent decades in the 20th century resisting calls for regulation, but today there is broad appreciation of the essential role that regulations have played in ensuring ubiquitous seat belts and air bags and greater fuel efficiency. The same is true for air safety, foods and pharmaceutical products. There will always be debates about the details, and the details matter greatly. But a world with vigorous regulation of products that are useful but potentially troubling is better than a world devoid of legal standards.

In 2005, Microsoft called for national privacy legislation for the United States in 2005 and they have supported the General Data Protection Regulation in the European Union. Consumers will have more confidence in the way companies use their sensitive personal information if there are clear rules of the road for everyone to follow. While the new issues relating to facial recognition go beyond privacy, Microsoft believes the analogy is apt.

It seems especially important to pursue thoughtful government regulation of facial recognition technology, given its broad societal ramifications and potential for abuse. Without a thoughtful approach, public authorities may rely on flawed or biased technological approaches to decide who to track, investigate or even arrest for a crime. Governments may monitor the exercise of political and other public activities in ways that conflict with longstanding expecta-

tions in democratic societies, chilling citizens' willingness to turn out for political events and undermining our core freedoms of assembly and expression. Similarly, companies may use facial recognition to make decisions without human intervention that affect our eligibility for credit, jobs or purchases. All these scenarios raise important questions of privacy, free speech, freedom of association and even life and liberty.

So what issues should be addressed through government regulation? That's one of the most important initial questions to address. As a starting point, Microsoft believes governments should consider the following issues, among others:

- Should law enforcement use of facial recognition be subject to human oversight and controls, including restrictions on the use of unaided facial recognition technology as evidence of an individual's guilt or innocence of a crime?

- Similarly, should we ensure there is civilian oversight and accountability for the use of facial recognition as part of governmental national security technology practices?

- What types of legal measures can prevent use of facial recognition for racial profiling and other violations of rights while still permitting the beneficial uses of the technology?

- Should use of facial recognition by public authorities or others be subject to minimum performance levels on accuracy?

- Should the law require that retailers post visible notice of their use of facial recognition technology in public spaces?

- Should the law require that companies obtain prior consent before collecting individuals' images for facial recognition? If so, in what situations and places should this apply? And what is the appropriate way to ask for and obtain such consent?

- Should we ensure that individuals have the right to know what photos have been collected and stored that have been identified with their names and faces?

Should we create processes that afford legal rights to individuals who believe they have been misidentified by a facial recognition system?
This list, which is by no means exhaustive, illustrates the breadth and importance of the issues involved. Another important initial question is how governments should go about addressing these questions. In the United States, this is a national issue that requires national leadership by our elected representatives. This means leadership by Congress. While some question whether members of Congress have sufficient expertise on technology issues, at Microsoft they believe Congress can address these issues effectively. The key is for lawmakers to use the right mechanisms to gather expert advice to inform their decision making. In the past Congress has appointed bipartisan expert commissions to assess complicated issues and submit recommendations for potential legislative action. Such commissions are "formal groups established to provide independent advice; make recommendations for changes in public policy; study or investigate a particular problem, issue, or event; or perform a duty." Congress' use of the bipartisan "9/11 Commission" played a critical role in assessing that national tragedy. Congress has created 28 such commissions over the past decade, assessing issues ranging from protecting children in disasters to the future of the army.

Congress should consider creating a bipartisan expert commission to assess the best way to regulate the use of facial recognition technology in the U.S. This should build on recent work by academics and in the public and private sectors to assess these issues and to develop clearer ethical princi-

ples for this technology. The purpose of such a commission should include advice to Congress on what types of new laws and regulations are needed, as well as stronger practices to ensure proper congressional oversight of this technology across the executive branch. Issues relating to facial recognition go well beyond the borders of the United States. The questions listed above – and no doubt others – will become important public policy issues around the world, requiring active engagement by governments, academics, tech companies and civil society internationally. Given the global nature of the technology itself, there likely will also be a growing need for interaction and even coordination between national regulators across borders.

Tech sector responsibilities

The need for government leadership does not absolve technology companies of their own ethical responsibilities. Given the importance and breadth of facial recognition issues, Microsoft and throughout the tech sector have a responsibility to ensure that this technology is human-centered and developed in a manner consistent with broadly held societal values. Many of these issues are new and no one has all the answers. It is incumbent upon those in the tech sector to continue the work needed to reduce the risk of bias in facial recognition technology. No one benefits from the deployment of immature facial recognition technology that has greater error rates for women and people of color. One must recognize the importance of collaborating with the academic community, other companies, including in groups involved with Artificial Intelligence, and a variety of external stakeholders, including customers, security interests, human rights and privacy groups that are focusing on the specific issues involved in facial recognition. One must recognize that one of the difficult issues to address is the distinction between the development of facial recognition services and the use of broader IT infrastructure by third parties that build and deploy their own facial recognition technology. The use of infrastructure and off-the-shelf capabilities by third parties are more difficult for a company to regulate, compared to the use of a complete service or the work of a firm's own consultants, which readily can be managed more tightly.

Microsoft's Smith recognized the importance of going more slowly when it comes to the deployment of the full range of facial recognition technology. He pointed out that "many information technologies, unlike something like pharmaceutical products, are distributed quickly and broadly to accelerate the pace of innovation and usage. 'Move fast and break things' became something of a mantra in Silicon Valley earlier this decade. But if we move too fast with facial recognition, we may find that people's fundamental rights are being broken." His company has turned down some customer requests for deployments of facial recognition services where it has concluded that there are greater human rights risks and monitor the potential uses of its facial recognition technologies with a view to assessing and avoiding human rights abuses.

In a similar vein, we're committed to sharing more information with customers who are contemplating the potential deployment of facial recognition technology. We will continue work to provide customers and others with information that will help them understand more deeply both the current capabilities and limitations of facial recognition technology, how these features can and should be used, and the risks of improper uses.

Fourth, we're committed to participating in a full and responsible manner in public policy deliberations relating to facial recognition. Government officials, civil liberties organizations and the broader public can only appreciate the full implications of new technical trends if those of us who create this technology do a good job of sharing information with them. Especially given our urging of governments to act, it's incumbent on us to step forward to share this information. As we do so, we're committed to serving as a voice for the ethical use of facial recognition and other new tech-

nologies, both in the United States and around the world.

We recognize that there may be additional responsibilities that companies in the tech sector ought to assume. We provide the foregoing list not with the sense that it is necessarily complete, but in the hope that it can provide a good start in helping to move forward.

Some concluding thoughts on technology

As one thinks about the evolving range of technology uses, it is important to acknowledge that the future is not simple. A government agency that is doing something objectionable today may do something that is laudable tomorrow. We therefore need a principled approach for facial recognition technology, embodied in law, that outlasts a single administration or the important political issues of a moment. Even at a time of increasingly polarized politics, we have faith in our fundamental democratic institutions and values. We have elected representatives in Congress that have the tools needed to assess this new technology, with all its ramifications. We benefit from the checks and balances of a Constitution that has seen us from the age of candles to an era of artificial intelligence. As in so many times in the past, we need to ensure that new inventions serve our democratic freedoms pursuant to the rule of law. Given the global sweep of this technology, we'll need to address these issues internationally, in no small part by working with and relying upon many other respected voices. We will all need to work together, and we look forward to doing our part.

Employers Beware: ICE ramping up I-9 audits to record levels

More than 5,200 businesses in the U.S. have been served with I-9 inspection notices since January in a two-phase nationwide operation conducted by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) in what appears to be the largest I-9 inspection action ICE has undertaken to date.

This latest round of workplace audits on employers clearly indicates that the I-9 inspection is now a top priority in U.S. immigration enforcement policy that targets employers rather than employees via the workplace raids of the past.

This alert, provided to ISPLA by the labor employment law firm of Fox Rothschild, outlines the current processes in place for I-9 inspections and includes practical advice on how to respond to an audit as well as steps to take now to ensure that your business is in compliance.

Notice of Inspection – NOI

The inspection process begins with HSI serving a Notice of Inspection (NOI) on an employer, which informs them that HSI will perform a comprehensive review of (i.e. audit) their hiring records (specifically Form I-9s and associated documents) to determine compliance with employment eligibility verification laws. Upon receiving an NOI, an employer is required to produce the company's I-9s within three business days, after which ICE will conduct an inspection for compliance.

In Phase I of the current operation, between Jan. 29 and March 30, 2018, HSI served 2,540 NOIs and made 61 arrests. During Phase II, between July 16 and 20, HSI served 2,738 NOIs and made 32 arrests.

ICE is the federal agency responsible for upholding the Immigration Reform and Control Act (IRCA), a law designed to protect jobs for U.S. citizens and others who are lawfully employed, eliminate unfair competitive advantages for companies that hire an illegal workforce, and strengthen public safety and national security.

Under IRCA, employers are required to verify the identity and employment eligibility of all individuals they hire, and to document that information using the Employment Eligibility Verification Form I-9. ICE/HSI uses the I-9 inspection program to promote compliance with the law, part of a comprehensive strategy to address and deter illegal employment. Inspections are one of the most powerful tools the federal government uses to en-

sure that businesses are complying with U.S. employment laws.

A 'Culture of Compliance'

Derek N. Benner, Acting Executive Associate Director for HIS, stated: "Employers need to understand that the integrity of their employment records is just as important to the federal government as the integrity of their tax files and banking records. All industries, regardless of size, location and type are expected to comply with the law."

Benner contends that worksite enforcement "protects jobs for U.S. citizens and others who are lawfully employed, eliminates unfair competitive advantages for companies that hire an illegal workforce, and strengthen public safety and national security."

HSI increased the number of I-9 audits, Benner said, to "create a culture of compliance among employers."

All employers in the United States are required to have a Form I-9 on file for all employees to verify their identity and authorization to work in the United States. The law requires that employers execute this process upon hire of an employee, review and record the individual's original, valid identity documents and determine whether those documents reasonably appear to be genuine and related to the individual.

HSI follows a detailed process when conducting a Form I-9 inspection. Guidance on that process and the associated civil fine structure can be found here. This guidance outlines ICE's process for a Form I-9 inspection, the penalties for various related violations, and the factors ICE considers during the course of the inspection and in determining a fine, including mitigating or enhancing factors involved.

Civil Fines and Potential Prosecution

Employers determined not to be in compliance with the law face the likelihood of civil fines and could ultimately face criminal prosecution if it is determined that they were knowingly violating the law. All workers encountered during these investigations who are unauthorized to remain in the United States are subject to administrative arrest and removal from the country.

Failure to follow the law can result in criminal and civil penalties. In FY17, businesses were ordered to pay $97.6 million in judicial forfeitures, fines and restitution, and $7.8 million in civil fines, including one company whose financial penalties represented the largest payment ever levied in an immigration case.

Monetary penalties for substantive and uncorrected technical violations, errors that the layperson often view as 'paperwork errors' range from $220 to $2,200 per violation and penalties for knowingly hiring and continuing to employ violations range from $3,548 to $19,242 per violation. In determining penalty amounts, ICE imposes a higher fine rate on employers with a higher percentage of I-9s with violations and then considers five factors to either enhance or mitigate fine amounts: the size of the business, good faith effort to comply, seriousness of violation, whether the violation involved unauthorized workers and history of previous violations.

What to Do if the Government Wants to Inspect Your I-9s:

- Call your immigration attorney immediately. The time period for responding to ICE is short and it is critical that documents submitted in response to the notice be well-organized and presented in the best light possible.
- DO NOT submit any documents to ICE without seeking the advice of counsel.
- DO NOT consent to an immediate inspection if agents show up without warning. You have up to three days to respond/submit documents.
- DO NOT submit more than what is asked for (such as expired I-9s for former employees, payroll records listing employees not subject to the inspection, etc.)
- DO NOT let agents take original records without permitting you to take copies
- DO NOT allow officers to talk with any employees or company officers before you call your attorney.
- If Department of Labor agents show up for an inspection without notice, decline the inspection. They will notify USCIS/ICE.
- DO NOT panic and try to correct or otherwise repair your records without the assistance of qualified immigration counsel. Corrections made or new I-9s prepared

after the issuance of an NOI are not accepted by ICE, and may create the appearance of bad faith.

The Tools of Protection

Employers that have not yet received an NOI should take immediate steps to protect against possible future violations.

Two key tools in ensuring IRCA compliance are private internal audits and specialized training. Employers should conduct private internal audits with the assistance of a qualified immigration professional to review I-9 documents and correct any errors in advance of an inspection. This type of periodic audit can not only uncover problems in time to be corrected before the imposition of sanctions, but can also demonstrate the employer's good faith efforts to comply with IRCA's verification requirements, a mitigating factor in ICE's penalty determination process. Because private I-9 audits can be performed over time and at the employer's convenience, it is less arduous for a company than the three-day audit period forced by an inspection notice.

Although employers can select from a variety of service providers to meet their I-9 audit and training needs, legal professionals with experience with immigration, employment and labor law are better equipped to handle IRCA compliance issues, including audits, training and formal inspections. Fox Rothschild provides companies of all sizes with IRCA compliance training seminars and confidential, internal I-9 audits.

Alka Bahal, *the author of this alert, is a Partner and Co-Chair of the Immigration Practice of Fox Rothschild, focusing on corporate immigration law and compliance and may be reached at (973) 994-7800 or abahal@foxrothschild.com.*

U.S. Foreign Corrupt Practices Act (FCPA): Third-party agents' payments violating anti-bribery law

French aircraft manufacturer Airbus SE has disclosed it may have violated U.S. law on fees and commissions paid to sales agents. The U.S. now believed to be conducting a probe along with ongoing U.K and French investigations. The firm informed authorities that their filings with the U.S. State Department contained certain inaccuracies and that they are cooperating with the three investigations being conducted. This case stresses the importance of properly vetting third-party agents, although there can be value in hiring an agent in a country with local expertise. In a January 2018 corpcounsel.com article, Neil Smith of K&L Gates, previously with Enforcement Division of the SEC, recommended due diligence follow these steps: (1) determine why the agent is especially qualified for the assignment, look for any past impropriety and connection to a government official (2) have agent sign a contract that warrants no bribery laws will be violated and be certain amount of payment is commensurate with the work being done (3) know what the agent is doing to market the company's product and monitor same (4) have company's legal and compliance officials sign-off on the agent, and (5) do not allow agent to hire other representatives or subcontractors without proper vetting.

Federal Trade Commission 2017 Annual Report

The FTC has released its annual report summarizing its privacy and data security work in 2017. The Commission is the nation's primary privacy and data security enforcer and one of the most active privacy and data security enforcers that can present legal exposure to the professional investigator who is not up to date on this agency's enforcement power.

The Commission uses a variety of tools to protect consumers' privacy and personal information, including bringing enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. Among the FTC's privacy and security actions announced in 2017 included settlements with computer manufacturer Lenovo and Vizio, one of the world's largest makers of smart TVs. In addition, the FTC in 2017 brought its first actions enforcing the EU-U.S. Privacy Shield framework.

The Commission's privacy accomplishments continue in 2018. The FTC announced the agency's first children's privacy and security case involving connected toys against electronic toy maker VTech. The company agreed to pay $650,000 to settle allegations that it violated the Children's Online Privacy Protection Act by collecting personal information from children without providing direct notice and obtaining their parent's consent, and failing to take reasonable steps to secure the data it collected. Also this year, the FTC and the state of Nevada charged the revenge porn site MyEx.com with violating federal and state law by posting intimate images of people, together with their personal information, without their consent.

ID Theft

The ABA Journal Series *Cybersecurity and the law* provided the following checklist. It comes with the usual disclaimer that you should engage in a threat assessment of your own situation in order to know the best way to protect your data. Further, these are not foolproof recommendations. Nevertheless, if you are not doing the things below, you are likely less safe for it.

1. Have you been pawned? It is pretty safe to say we have all been hacked or compromised at this point. Between the breaches of Equifax, LinkedIn and Yahoo, information from billions of accounts have spilled out into the world. But were you one of them? While it is impossible to be 100 percent certain, there is one way to see if your account information has fallen prey to a hack. By going to haveibeenpwned.com, you can type in your email addresses or usernames to see if they come up in the sites database of publicly known hacks. If a hack has occurred but it has not been verified or made public, then the site will not have that information. However, it is a good first step to know if your passwords have been compromised.

2. Consider a password manager. If your email address came up on "haveibeenpwned," your palms are probably sweaty and fear has overtaken you. This is normal, but not necessary. Let us channel that nervous energy towards getting serious about passwords. Even the grinning readers who did not see their email on the website should follow along. A password manager will help you store your bevy of passwords, which should all be as unique as a snowflake. No longer will you need gimmicks to remember which password had an exclamation point or the capital "T" in it. The manager will handle that for you. While not hocking particular software, the Electronic Frontier Foundation has some handy questions to vet a company promising you security:

- Is the company clear about the limitations of its product? Do not trust companies that promise the world or use buzzwords like "military grade." That is gibberish and should be discounted.
- Does the company share its threat model in case of a compromise? Mature companies who trust in their product will be transparent about the attacks they are prepared for and how they are prepared. Look for this documentation.
- Does the company say it cannot or will not access your data? You might have to read the terms of service, but companies that cannot access your data by design are better. "Will not" leaves the backdoor ajar.
- What do users say? Like everything else, you can find online reviews of password managers. Do people still trust the tool? Has the company made unfortunate headlines recently? These are all things to consider in your decision.
- When you are thinking about which manager to use, Princeton's Center for Information Tech-

nology Policy found that the password managers that come default in many browsers are being used by ad trackers to scoop up your data.

3. Treat yourself to better passwords. It is 2018, and a password under seven characters that combines your dog's name and your birth year are not sufficient. Nor is it cool that you have a dozen passwords that are permutations of each other. The National Institute of Standards and Technology updated their password guidelines last year, and they recommend that you create a strong password, or longer passphrase where possible, that avoids the maddening nature of passwords with upper-case, special symbols and numbers. Think of a line from a book or song that is not that popular and easy for you to remember. This is especially important to master passwords to things like that new password manager you got after reading this article. Also, unless you are breached, NIST no longer recommends making periodic changes to your password. If it is not broke, do not fix it. Last, NIST recommends avoiding password hints or knowledge -based authentication, which brings us to…

4. Two-factor authentication! Congratulations if you thought to yourself, "I already do that." If so, you've graduated to step five. However, if you do not know what two-factor authentication is, keep reading. Two-factor authentication is a two-step process to signing into an account. Instead of merely typing your password and logging in, two-factor will send you an email or text message with a unique passcode to enter before you can access your account. The hope here is that if your password is compromised, you have a second line of defense. All major companies have two-factor now, so take advantage of it. (For a list of sites with two-factor authentication check out twofactorauth.org.)

5. Encrypt your devices. Encryption has become a painless, low cost way to protect your information. Doing so can make you feel slightly more secure if you lose or misplace your device. Android, Apple and Microsoft now all have turnkey encryption for their devices. For Android Pixel, Samsung Galaxy S8 and later phones, they come encrypted. For iPhone users, it is as easy as turning on your passcode, which Apple says 89 percent of its customers already do. Windows, as well, makes it easy to turn on Bit Locker, their encryption service. With this step, do not forget to also encrypt external storage devices you use for documents.

Contact Bruce at brucehulme@yahoo.com . Please donate to ISPLA to assist in its continuing mission.

♦♦♦

Cyberextortion Legal Implications Seminar

Cyber extortion has reached new proportions, including six-figure ransomware payments. Considering cyberextortion payoffs, cybersecurity experts expect these attacks to only increase. On September 12, 2018, 6:00pm-8:00pm, the New York Chapter of the ACFE will have as its evening dinner speaker Ondrej Krehel, an expert on such subjects. The event will be held at the Battery Gardens (inside Battery Park opposite 17 State Street). This session will explore the legal implications of a current attacks for sectors such as healthcare, financial, and others. Issues include OCR's proposal of treating a ransomware attack as a data breach, GDPR, various States and SEC actions, as well as practical advice for how to deal with various matters that emerge as a result of an attack. Legal, Regulatory and Forensic will meet in one this discussion to holistically debate challenges, issues and caveats during cyber extortion attack. **Attendees will be entitled to 2CPE credits**. ***FULL 3-course Dinner with attendance including FREE*** *Wine, Beer & Soda & hors d'oeuvres.* **NYCFE Member Price $35** (Special member rate subsidized thanks to LIFARS). **Non-NYCFE Members: $75. REGISTER EARLY TO RESERVE YOUR SEAT.** *The NYCFE is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE.* Go to: https://nycfe.starchapter.com/meet-reg1.php?mi=1024934&id=83.