



INTELLENET *News*

Official Newsletter of the
International Intelligence Network, Ltd.

Intellenet.org

Winter 2019

In this Issue ...

PETER'S POSTING

2

WELCOME NEW MEMBERS

2

MEMBER NEWS

3

CRYPTOCURRENCY: AWARENESS & RECOGNITION

5

ISPLA & INTELLENET: ADDRESSING GLOBAL REGULATORY & LEG- ISLATIVE ISSUES

7

ISPLA INSIGHTS

8

THE FBI SAYS ITS PHOTO ANALYSIS IS SCIENTIFIC EVI- DENCE. SCIENTISTS DISAGREE.

10



Peter's Posting

by
Peter Psarouthakis
Executive Director



***“It’s not too late to register for
Intellenet’s 2019 conference ...”***

***Our 2019 conference in
Charlotte, NC from April
2-5 is right around the corner. It is
not too late to register.***

Go to the Intellenet [website](#) and you will find all the conference information you need. This is going to be another not to be missed event. Conference hosts Don and Gina Hubbard have been working hard with

our conference committee to make this conference fun, memorable and educational. Speaking of education, our director of education Jeff Stein has put together a very strong program. CEU credits will be awarded that can be used for licensing and certifications you may need. Contact [Jeff Stein](#) for all your CEU questions. General conference questions should go to [myself](#) or [Ed Spicer](#).

At this year’s conference we also will be holding our annual board of directors meeting. The board is

working hard on items such as membership recruitment, marketing the membership to potential clients and providing the best possible conference experience each year. Intellenet was an exhibitor at several conferences in 2018, in order to promote our members to potential clients, and we will continue that effort in 2019 and beyond. Driving potential clients to our website when they need investigation and

security services is a high priority for the board. Of course, the association would not be anything without its members. We are always looking for qualified members throughout the world. If you know of a qualified person please send us their name and contact information so that we can help recruit them into our ranks.

We look forward to seeing everyone in Charlotte!



Welcome New Members!

Jan BAREFOOT — Charlotte, NC

Jose CALDERON — Corpus Christi, TX

Gabriele CONFLITTI — Hamilton, Ontario CANADA

Randy DOWNER — Tucson, AZ

Steve FOX — St Louis, MO

Max FRATODDI — Bluffton, SC

Toine GOORTS — Helmond, NETHERLANDS (reinstated)

Michael JULIAN — Murrieta, CA

Alexander KRIONI — Moscow, RUSSIAN FEDERATION

Dave MacNEIL — Watertown, MA

Lori MILLER — Bend, OR

Lynette REVILL — Sarasota, FL (reinstated)

Peter SNELL — GUATEMALA

Willem TEUBEN — CURACAO

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.

★ Member News ★

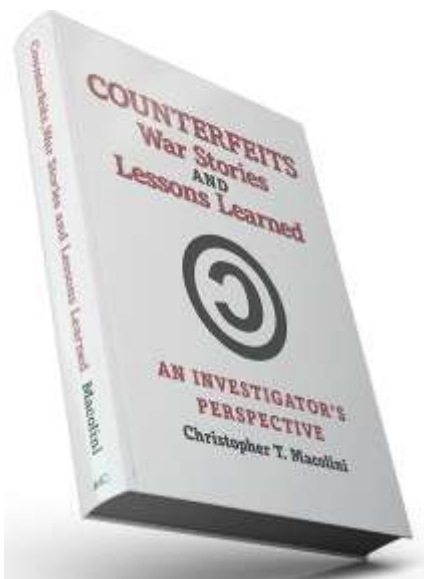
Remi Kalacyan and his firm, VIP Investigations, Inc. of Montreal, Quebec, Canada won the city's prestigious Consumer Choice Award, Investigator of the Year for 2019. Congratulations, Remi!



Phil Johnson, right, with Bob Bridgestock, co-author with wife Carol of the novels featuring "... my favourite DI Jack Dylan ..." Bob was a senior detective with the West Yorkshire Police. Bob and Phil are celebrating the launch of the latest in the series, "Poetic Justice."

Member News continues next page ...

PRESS RELEASE



In *Counterfeits, War Stories and Lessons Learned*, **Christopher T. Macolini** provides brand owners and investigators with a proven roadmap for combatting these threats. Using a mix of practical advice and descriptions of his real-life professional experiences, Chris presents invaluable information for brand owners and investigators at all levels of skill to conduct successful campaigns against those who threaten the hard-won value of brand-name products and their owners.

Christopher T. Macolini has a wide variety of investigative skills gleaned from over 30 years of experience with both U.S. federal law enforcement, as well as private sector investigations.

Chris is a partner with MIC Worldwide LLC, a bespoke global risk consultancy that specializes in helping organizations understand and manage risks when operating in complex environments. He is an accomplished speaker, a published author and certified life coach.



Kevin McClain, CCDI, BAI recently announced the initial launch of his mobile application connecting investigators and clients in real time scenarios at accident and incident sites. The launch is scheduled for April 1, 2019 and it's not too late to sign up ...

All Intellenet members who sign up before launch date will be grandfathered in and will never have a subscription fee!

Kevin already has over 450 investigators in his investigative network and clients are signing up for beta testing. The Phase 1 Launch in April will offer the app to over 300,000 truckers as apart of a strategic agreement with the trucking industry, offering real-time local investigative expertise at accident sites via the app's instant notification capabilities.

If you are ready to be a part of this exciting network or have any questions about READI Response, contact Kevin at 877-532-1152 or email mcclainpi@gmail.com or kevin.mcclain@readiresponse.com.





“Cryptocurrency” Awareness and Recognition

What is “cryptocurrency”?

“Cryptocurrency” is a peer-to-peer digital currency with no central administrating authority that uses cryptography to verify transactions and secure the historical record of transactions. That record (which excludes real-world identities of people transacting) is maintained via the Internet in a distributed public ledger called a “blockchain.” Criminals often use cryptocurrency instead of cash or other monetary instruments. Information about its use can help investigators identify suspects and co-conspirators, “follow the money,” and seize funds.

Common types

Bitcoin



Ethereum



Litecoin



Ripple



Dash



Monero



Zcash



“Addresses” and “Private Keys”

An “address” or “public address” is a long string of letters and numbers, often shown as a QR code, that represents a digital record where cryptocurrency can be sent or stored.

Bitcoin Address



SHARE

1KYNhhMRBboMYpL4X1rnLHATetZ8wK9R2U

A “private key” is a different alphanumeric string (or QR code) that is paired with an address and represents the secret information used to digitally sign a transaction. This is how funds are transferred/spent from that address, which can be done by anyone who has this key.

Private Key

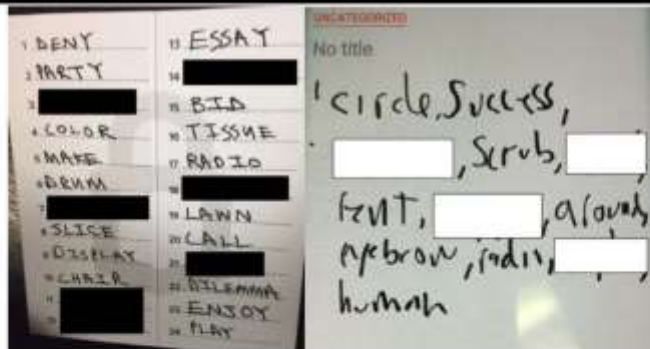


SECRET

KxFDQ6NKyFo6SAqAARukQB9caDuG1gKCHN1jyAZpXi4A2FnN8dh

“Recovery seed” or “Mnemonic phrase”

A type of private key expressed as a string of seemingly random words (typically 12 - 25). The words are the human readable form of a complex “root private key” that generates a certain set of address/key pairs. The recovery seed can be used to regenerate an identical copy of a “wallet” (see below) because that set of words creates the same set of address/key pairs every time it is entered into certain software. You may find them written down.



Can cryptocurrency be seized?

Like other assets, cryptocurrency can be seized. This is done by gaining access to the “wallet” (i.e., the private keys) and transferring the crypto from the suspect’s wallet into an address/wallet controlled by a law enforcement agency.

“Cryptocurrency” continues on next page ...





ISPLA & INTELLENET Addressing Global Regulatory & Legislative Issues

by
BRUCE H. HULME, CFE, BAI



I have acted as the INTELLENET Legislative Liaison Board member for several decades as well as ISPLA's Director of Government Affairs now for the past decade. Both organizations have a joint agreement presently in place that effectively allows ISPLA to represent INTELLENET's interests in legislative and regulatory affairs, both nationally and internationally.

Each year I write four articles on this subject and other items of possible interest to investigative and security professionals in *INTELLENET's e-newsletter* and six articles in *PI Magazine* of a similar nature. In the past three issues of *PI Magazine*, my articles have emphasized the close relationship of the two organizations. The ISPLA column has been published (as has that of NCISS) in *PI Magazine* under the previous ownership of Jimmie and Roe Meis and now the new publishers, Nicole Cusanelli and James Nanos. I was formerly an associate editor at that magazine during the five years that I served as the NCISS Legislative Director and wrote a similar column in each issue during those years as well.

I am prepared to continue writing such articles under a proposed joint ISPLA/INTELLENET legislative and regulatory initiative and believe consideration should also be given offering ISPLA's members *who qualify* to be merged into

INTELLENET. This action could conceivably increase the membership of INTELLENET 50 percent overnight. With regard to the future of ISPLA, it is my hope that our decade affiliation with INTELLENET will continue its mission under the auspices and leadership of INTELLENET

as I wind down much of my legislative affairs activity--except for special instances where my expertise might be of value to my investigative and security professional colleagues.

I have served as a legislative advocate, officer or board member on behalf of our profession's associations for over five decades with ALDONYS, three with NCISS, and more than two each with IASIR, INTELLENET, SPI, NY Chapter ACFE, John Jay College of Criminal Justice, and as a gu-

bernatorial appointee of the NY State Security Advisory Council. Over the years, I have helped build alliances with colleagues, stakeholders, key legislators, and regulators. I believe that it is now time for those of you supporting me to take the lead in continuing this work. In my opinion, along with other colleagues with whom I have discussed this matter, INTELLENET is the best professional association to address future legislative and regulatory issues at both the U.S. and international levels.

“With regard to the future of ISPLA, it is my hope that our decade affiliation with INTELLENET will continue its mission under the auspices and leadership of INTELLENET ...”





ISPLA Insights for INTELLINET

by

BRUCE H. HULME, CFE, BAI

ISPLA Director of Government Affairs

The GDPR, artificial intelligence, security breaches, privacy and the "Russians" will no doubt continue to be hot topic issues into 2019 that will have unintended consequences for investigative and security professionals. In the new two-year 116th Congress, the Democratic

House will re-offer privacy bills that failed in the 115th Congress. I expect major corporations to continue to push for federal preemption on data breach security and privacy bills. Our profession's position will become tenuous due to the financial resources of such businesses and their lack of general knowledge of how records closure and elimination of our sources of information

actually affect their own industries. The major credit bureaus and other aggregators of personal information, along with emerging Artificial Intelligence (AI), will also impose restrictions upon our profession. Privacy advocates will increase their efforts to pursue their agendas and as such will be aided by examples of the government's increased use of surveillance and technologies upon its citizens in the name of Homeland Security. Isolated abuses by private sector investigators will continue to gain wide media attention and present opportunities for lawmakers to put forth detrimental measures in Congress. I envision that Congress or the Federal Trade Commission will continue to classify private investigators as information brokers in legislation or regulation.

Facebook, Google, Microsoft, and others have expressed

their concerns over far-reaching and often conflicting privacy bills expected to be offered and are aware that the public's confidence in the Internet and emerging technologies such as facial recognition and geolocational monitoring is fading. Notwithstanding the current administration's push to eliminate federal regulations, businesses are still frustrated with the growing number of privacy measures and proposed industry-specific laws that make compliance cumbersome without easing consumer fears and distrust.

"The major credit bureaus and other aggregators of personal information ... will also impose restrictions upon our profession."

These high-tech companies will push for federal measures that supersede California's 2018 law with a more "industry-friendly" federal bill. Some members of Congress will seek to replicate measures along the lines of Europe's General Data Protection Regulations. The bipartisan backlash to Congressional testimony given during 2018 by executives such as Facebook's Mark Zucker-

berg, makes it possible that such a regulation could be reached. It is likely that some type of privacy legislation will pass. The exact contours of that legislation will no doubt be the subject of debate among lawmakers, lobbyists, and privacy advocates in the months to come.

When Facebook was first accused of misleading customers about their privacy in 2011, it entered into a consent decree with the Federal Trade Commission, promising not to do it again. However, when Facebook found out about Cambridge Analytica, it failed to pass on their findings to the FTC. The FTC is now investigating Facebook, but the incident suggests that the agency's existing enforcement mechanisms are at best flawed. Independent counsel Robert Mueller's investigation has revealed Russia's role in the 2016 election—indictments around past Russian business deals and money laundering; indictments of Russia's Internet Research Agency for its information-influence

operations on Twitter, Facebook, and other social media sites; indictments of Russian military intelligence officers for the theft and publication of Democratic emails, and an attack on state-level voting systems; and then indictments of Trump campaign officials for lying about their contacts with Russian officials.

Below are just some of the topics that will affect our INTELLENET international members as well as those in the U.S.

California's Consumer Privacy Act (CCPA), signed into law in 2018, follows a growing line of consumer privacy laws, such as the European General Data Protection Act (GDPR), Canadian Breach of Security Safeguards Regulations of the Personal Information Protection and Electronic Documents Act (PIPEDA), and related New York Department of Financial Services Cybersecurity Rules and Regulations (NYCRR-500).

As New York's NYCRR 500 regulations serve as the gold standard for cybersecurity protocols, California's CCPA will likely serve as the U.S. standard for privacy. Like its European GDPR counterpart, California's privacy act establishes consumer rights and corporate responsibilities, which will be enforced with penalties up to \$7,500 per violation. As motivation for the law, the California Act notably cites the tens of millions of people whose personal data was misused by the data mining firm Cambridge Analytica, a greater desire to heighten data privacy controls and transparency of data practices, and the people's de-

sire for privacy and more control over their information. The Act, which becomes effective on Jan. 1, 2020, could have a serious impact on the economic models of many companies collecting and reselling data to other parties. Transparency in data movement and resale will open the eyes of consumers who, until now, blindly



agree to user contracts and never question why an app on their phone needs access to their location, contacts, or other services.

Some of the Acts specific provisions include:

- Full disclosure regarding the collection of personal information, including details of the collected information, sources, the purpose, whether the data is disclosed or sold to another party, and if so, the third party's details.
- An opt-out right to prevent a business from selling their personal information to third parties.
- The right to be deleted (like with GDPR's right to be forgotten) by having their information wiped-off servers.

The Act mandates traceable transparency of consumer data collection, use, distribution, and the GDPR-like right to be forgotten. These requirements must be made public through

general policy, by specific request, and cannot form the basis of bias or discrimination on the part of the business. A company cannot tie goods or services to the ability to resell consumer information or offer discounts or other incentives in exchange for this ability. This moves consumer privacy rights from the domain of *often ignored* fine print to the front page.

The General Data Protection Regulation (GDPR) now in force among European Union country members, among other provisions, mandates that companies notify data-holders of a breach within 72 hours. It also gives E.U. residents the

"right to be forgotten" by having their data wiped off a company's servers. In the U.S., there is no comparable federal law that governs how all states handle data breaches and protects consumers' information. As it stands now, each of the states have different breach notification requirements, but the majority do not have sweeping legislation on the books on how companies handle personal data.

A national data privacy law offered by U.S. Rep. Hank Johnson, Jr. (D-4-GA), comes with the expected reintroducing of two measures that previously failed in the Republican-controlled House. The first bill, the Application Privacy, Protection and Security Act of 2018 (H.R. 6547), is meant to govern the use of personal data on mobile devices. Another, the DATA Act of 2018 (H.R. 6548), would allow U.S. citizens to have their data erased from corporate servers, and will make it easier for consumers to opt out of having their data used by third-

party collectors.

Johnson believes the bills did not pick up traction in the past because of an anti-regulatory environment in Congress. However, he said that because of the recent high-profile data breaches, they may be more likely to pass this time around and provide uniform rules for all 50 states.

Senator Ron Wyden (D-OR), one of Congress's privacy advocates, has also circulated a draft bill that would expand the FTC's powers by establishing privacy and cybersecurity standards, while giving the FTC the power to fine companies for the first offense, which is not currently within its purview. "It's time for some sunshine on this shadowy net-

work of information sharing," he wrote. Senator Wyden also co-authored a bill that would require a court order to install a surreptitious GPS tracking system. In the previous sessions of Congress passage of this bill was opposed by ISPLA and others. His Republican sponsor has since left the Senate. I believe Senator Wyden will have little trouble gaining Republican sponsorship.

Bruce can be reached at
BruceHulme@yahoo.com



THE FBI SAYS ITS PHOTO ANALYSIS IS SCIENTIFIC EVIDENCE. SCIENTISTS DISAGREE.

The bureau's image unit has linked defendants to crime photographs for decades using unproven techniques and baseless statistics. Studies have begun to raise doubts about the unit's methods.

BY RYAN GABRIELSON, JAN. 17, 2019 IN



At the FBI Laboratory in Quantico, Virginia, a team of about a half-dozen technicians analyzes pictures down to their pixels, trying to determine if the faces, hands, clothes or cars of suspects match images collected by investigators from cameras at crime scenes.

The unit specializes in visual evidence and facial identification, and its examiners can aid investigations by making images sharper, revealing key details in a crime or ruling out potential suspects.

But the work of image examiners has never had a strong scientific foundation, and the FBI's endorsement of the unit's findings as trial evidence troubles many experts and raises anew questions about the role of the FBI Laboratory as a standard-setter in forensic science.

FBI examiners have tied defendants to crime pictures in thousands of cases over the past half-century using unproven techniques, at times giving jurors baseless statis-

tics to say the risk of error was vanishingly small. Much of the legal foundation for the unit's work is rooted in a 22-year-old comparison of bluejeans. Studies on several photo comparison techniques, conducted over the last decade by the FBI and outside scientists, have found they are not reliable.



Excerpt courtesy of ProPublica, "... an independent, nonprofit newsroom that produces investigative journalism with moral force." The complete article can be found at their [web site](#).

