# INTELLENET *News*

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

*Intellenet.org* *Spring 2019*

## *In this Issue . . .*



# Peter's Posting

*by*

***Peter Psarouthakis***
***Executive Director***

## Dear Intellenet Members:

# Do you have an "elevator speech"?

I hope that you are enjoying your spring so far and your business is going well. Intellenet continues to be strong in members worldwide, but we are always looking for qualified members. Which reminds me ...

I expect most of us know about elevator speeches. It's that short introduction of yourself to a stranger you happen to be sharing an elevator with. That's happened to me a number of times over the years during one of our conferences. In addition to introducing yourself, it's an ideal opportunity to talk briefly about Intellenet. But just as importantly it's a good speech to have ready when talking to a colleague who might be a good candidate for membership.

***"... it's a good speech to have ready when talking to a colleague who might be a good candidate for membership."***

Unlike any other investigation and security association, we require that new members have a minimum of 10 years of "investigative" experience. That experience does not have to come from just the private sector. Did you serve in a federal or state law enforcement before joining Intellenet? Do you know someone from your old agency that may now be working in the private sector and qualifies for membership? If so, please contact them about Intellenet. Let them know about your positive experiences since joining. Our members are the number one recruiting tool! And in the recruiting vein, we will continue this year to feature the Intellenet booth at conferences in an effort to identify qualified members.

Speaking of membership, the single biggest headache of any association is dues renewals. Having led several associations in my career, as well as speaking to other leaders of associations, I see that late renewals are a problem everywhere. I personally believe it is a cultural problem we as association members have created in all associations over a long time. Specific to Intellenet, we have a paid administrator who does an amazing job for our association handling many administrative duties, including renewals. Late renewals means that time (which means money) is being spent tracking down those members who are late. Also, is it fair to those members that pay on time to have to carry those non-paid members for months? The Board is discussing ways to handle this issue and in 2020 there will be a new policy in place. Thank you in advance for your cooperation in helping your association address this concern.

Our conference committee is hard at work putting together the 2020 conference at the Rio Resort and Casino in Las Vegas, Nevada. Information is available on the Intellenet website. We have some special events planned for the conference that you will not want to miss. More information to come soon.

Have a great summer!

♦♦♦

# Member News

## *Charlotte 2019: A conference for the times …*

This year's annual conference in Charlotte, North Carolina, was memorable in more ways than one, not the least of which was the annual dinner featuring a 1920's murder mystery. Several flappers, gun molls and shady characters were present, some seen here.

*"Flappers" Tina Blanchette, left, and Alice Cappiello.*

*"Killer" Steve Kirby, from, uh, Chicago …*

Intellenet's photographer, **Ed Kelly,** was on hand to capture these photos and many others, previously forwarded to the Intellenet-L and Intellenet-D email listservs, and posted on our website.

***Member News continues on next page …***

## *Member News ...*

*Conference 2019 "Gun moll and gangster," Dawn and Don Hubbard*

## Welcome New Members!

**Joshua ASKEW — Jacksonville, FL**

**Jeremy "Jax" ATWELL — Great Falls, MT**

**Justin BROWN — Pittsburgh, PA**

**Mark GILLISPIE (reinstated) — Austin, TX**

**Larry GOULD — Miami, FL**

**Paul JOHNSON — St. Louis Park, MN**

**Bob KRESSON (reinstated) — Pittsburgh, PA**

**Richard LINDBACK — Tucson, AZ**

**David NALLEY — Easley, SC**

**Rafael RUIZ — El Paso, TX**

**Paul SEGUIN — Raleigh, NC area**

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.

## *An Editor Signs Off ...*

My first issue as your editor was the Spring issue of 2012 and now, appropriately enough, with the Spring issue of 2019, I sign off, with special thanks to all of you for your support of our newsletter. I am especially grateful to those who have contributed to our Member News column, my favorite section of our quarterly. I enjoy seeing news of the many accomplishments of members and their firms. A special thanks to those who have shared articles and other items of interest. The most challenging task of any editor is gathering sufficient material for each issue. Ed Spicer will take over as editor with the Summer edition and your newsletter will be in good hands. Please show him the support you have shown me. Ed, thanks!

I am grateful for the support of my predecessor as editor, Bill Blake, whom I consider one of the best writers and editors in our profession. Bill's stewardship of getting the Intellenet books to market "raised the bar" on the Intellenet brand. I appreciate the support of the two Executive Directors I have served under, Jim and Peter. And last but not least, thank you, Bruce, for your regular columns on behalf of ISPLA and forwarding news of interest for those of us who share many interests and concerns in an ever changing international community.

I am most grateful for the invitation to join Intellenet, all those years ago. Thank you, Jim. But, hey, I'll be around for quite a while longer. I'm having trouble figuring out how to retire. I don't golf, I don't fish ...

♦♦♦

**LICENSED PRIVATE DETECTIVES ASSOCIATION OF MASSACHUSETTS, INC.**

## 2019 CONFERENCE
## September 13 & 14, 2019
## Hampton Inn Conference Center,
## 319 Speen St., Natick, MA

# *ATTENDEE REGISTRATION FORM*

Hotel Room rates for this event have been discounted at ***$114.00 per night if registered by August 13, 2019.***
For overnight accommodations, please call the **Hampton Inn at 508-653-5000 (**mention the LPDAM Conference)

**Full Registration (Members):**

- **Pre-registration thru April 30, 2019** **$225.00**
  **(conference fee & 2019 dues paid by 4/30/19-2020 dues WAIVED)**
- **Registration after April 30, 2019** **$275.00**

**Non-Member** **$300.00***

**If separate LPDAM Membership Application is submitted prior to seminar registration fee will be same as Members*

**PLEASE CHECK WHERE APPROPRIATE:**

☐ LPDAM member. ☐ Member of State/National Associations:_____

☐ Employee/Guest of Member. _____

☐ OTHER - Please state qualifications: _____

**METHOD OF PAYMENT:**

☐ Check Enclosed (Payable to LPDAM) ☐ PayPal go to www.LPDAM.org

**TOTAL DUE BY CHECK OR PAYPAL:** _____

LAST NAME: _____ FIRST NAME:_____

FIRM NAME: _____

ADDRESS: _____

CITY: _____ STATE: ____ ZIP: _____

TELEPHONE: _____ FAX: _____

E-MAIL: _____

**Mail to: LPDAM CONFERENCE REGISTRATION**
200F Main St., Suite 303, Stoneham, MA 02180
**QUESTIONS:** Call Ed Spicer 978-473-4154 or ed@oceanstatesinv.com

***AGENDA ON REVERSE SIDE***

***SPONSORS***

Yergey INSURANCE

REDLINE FORENSIC STUDIOS

eChatter

**LPDAM 2019 Conference Agenda as of 4/10/19**

**Friday September 13th**

| | |
|---|---|
| ***7:30-8:30 AM*** | *Registration & continental breakfast* |
| ***7:30 AM*** | *Trade show opens* |
| ***8:30-9:00 AM*** | *Opening remarks & welcome* |
| ***9:00-10:30 AM*** | *William Gillis, Gillis Investigations, & Eddie Dominguez, Dominguez Investigations, "Executive Protection 101"* |
| ***10:30-10:45 AM*** | *Break* |
| ***10:45–12:00 PM*** | *Robin Pinzone- "Branding your PI/Security Company thru Social Media"* |
| ***12:00-1:30 PM*** | *Lunch Speaker Former Boston Police Comm William Evans "Marathon Runner to Marathon Investigator"* |
| ***1:30-2:15 PM*** | *Elaine Gill, Gill Investigative Services, "Title IX & the College Campus Investigation"* |
| ***2:15-2:30 PM*** | *Break* |
| ***2:30-3:45 PM*** | *Greg Stewart, Office of the Secretary of the Commonwealth, "Public Records Presentation"* |
| ***3:45-5:00 PM*** | *Attorney David O'Connor- "Surveillance issues in Workers Comp cases" (exact title TBD)* |
| ***5:00-5:30 PM*** | *Sean Burke/Mike Pavone-"Legislative Update"* |
| ***5:30-7:00 PM*** | *Vendor Cocktail reception & Comedian Paul D'Angelo (Former Essex County ADA turned Comedian)* |

***Saturday September 14th***

| | |
|---|---|
| ***8:00-8:45 AM*** | *Continental breakfast & trade show* |
| ***8:45-10:00 AM*** | *Jamie Martin, Lawmate-USA, "Latest & Greatest in Covert Surveillance Equipment"* |
| ***10:00–10:15 AM*** | *Break* |
| ***10:15-12:15 PM*** | *Dan Loper, Granite State Intelligence, "Digital Forensics"* |
| ***12:15-1:15 PM*** | *Lunch* |
| ***1:15-2:30 PM*** | *Jay Groob, American Investigative Services, "Surveillance – Guideline and Standards"* |
| ***2:30-3:30 PM*** | *Bree Jones/Jason Young, Redline Forensic Studios, "Forensic Video Processing & Analysis"* |
| ***3:30-3:45 PM*** | *Break* |
| ***3:45-5:00 PM*** | *Michael Yergey, Yergey Insurance, "Risk Management & Business Insurance Issues"* |
| ***5:00 PM*** | *Door prizes-* ***MUST BE PRESENT TO WIN*** |

***SPONSORS***

**Press Release**

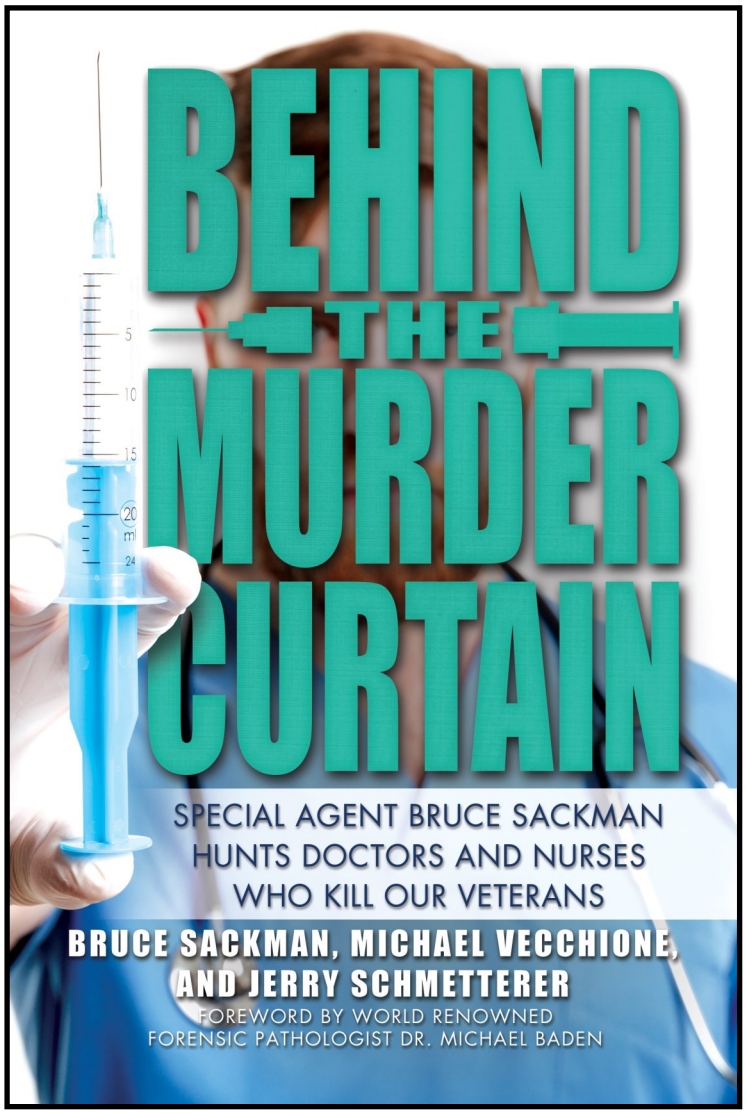
# Behind the Murder Curtain: Special Agent Bruce Sackman Hunts Doctors and Nurses Who Kill Our Veterans

*by*

## Bruce Sackman, Michael F. Vecchione, and Jerry Schmetterer

***Behind the Murder Curtain*** is the true story of **Bruce Sackman**, Special Agent in Charge of the Department of Veterans Affairs Office of Inspector General. Sackman's main responsibilities had been investigating white-collar crimes such as embezzlement when he is drawn into the macabre world of doctors and nurses who murder their patients. Sackman evolves from an investigator of routine cases to the world's leading expert on Medical Serial Killers—MSKs—doctors and nurses who ply their evil trade hidden behind the privacy curtain at a patient's bedside.

*Behind the Murder Curtain* tells how this dedicated investigator brought down four MSKs in Veterans Hospitals while developing THE RED FLAGS PROTOCOL, which is now taught to investigators and forensic nurses thorough out the world for stopping an MSK.




**About the Authors:**

**Bruce Sackman** served as the Special Agent in Charge, U.S. Department of Veterans Affairs, Office of Inspector General, Criminal Investigations Division, Northeast Field Office until May 2005 when he retired after 32 years' service. His cases have been featured on the Discovery Health Channel, CNN, MSNBC, *America's Most Wanted,* and on Home Box Office. **Sackman** is a member of Intellenet and self-employed as a licensed private investigator in New York City specializing in healthcare-related matters.

**Jerry Schmetterer** is an award-winning print and broadcast journalist. *Behind the Murder Curtain* is his sixth non-fiction book. He is a former bureau chief and editor at the *NY Daily News* and managing editor at CNN and WPIX in New York. He served for 12 years as spokesman for the Brooklyn District Attorney's Office. He is past president of the NY Press Club and currently serves as a Trustee. He lives in Manhattan with his wife, Emily.

**Michael Vecchione** is a former Chief of the Rackets Division of the Brooklyn District Attorney's Office, topping off his career of 40 years as a prosecutor. *Behind the Murder Curtain* is his third nonfiction book. He is a frequent contributor to true crime television productions as an expert on organized crime. He lives in Long Island City, NY, with his partner Lenor Romano.

***Available now on Amazon, Barnes & Noble and wherever books are sold.***

♦♦♦

# Intellenet's Board Accredited Investigator Program

Because private investigation is primarily an intellectual pursuit, it is more difficult to demonstrate your qualifications as an investigator, than it is for those individuals pursuing a hands-on career where your qualifications are demonstrated by your work product. Because of the lack of professional licensing in some states, an individual who completed an online investigation course can call themselves "private investigator" without any proof of their qualifications.

The Intellenet Board Accredited Investigator Program (BAI) has been established to demonstrate that the BAI accredited investigator has the necessary professional qualifications and experience. This is not an easy to achieve professional certification but is an excellent demonstration of the investigator's experience.

The qualifications are very stringent and only a limited number of investigators can obtain the BAI certification. There is a required minimum of 15 years of verifiable investigative experience. There are those who claim that the 15 year requirements is excessive; however, it is a true indication of the applicant's experience as Intellenet's goal is to enhance the professionalism of those with the BAI certification.

There is also a requirement for a 1000 or more word "White Paper" on an investigative topic that has not been previously published. A "White Paper" is an authoritative article as a demonstration of the applicant's experience. Additionally, the applicant must submit five questions derived from the White Paper for the BAI test databank.

Applicants will be required to successfully complete an on-line test on previously submitted White Papers which are available on the test site. Following the above actions, the applicant will be required to participate in a prearranged peer review.

The question may arise—"Why Become a Board Accredited Investigator"? The BAI designation is simply a total commitment to professionalism. Maintaining the BAI certification requires the investigator to be involved in a serious commitment to ongoing education which demonstrates that the private investigator is cognizant of current investigative laws, strategies, and techniques.

The BAI certification, through the auspices of Intellenet, is a unique credential specifically designed for professional investigators developed by practitioners for practitioners. Certification indicates mastery and competency as measured against a defensible set of standards acquired by application of stringent standards and examination.

## BAI Application Process & Requirements

♦

**BAI INFORMATIONAL TRIFOLD**

http://baipi.org/resources/Documents/BAI_trifold_6-8-19.pdf

**APPLICATION**

https://www.intellenet.org/bai/application-for-bai-designation/

**INFORMATIONAL WEBSITE**

www.BAIPI.org

♦♦♦


## ISPLA Insights for INTELLENET

*by*

**Bruce H. Hulme, CFE, BAI**
**ISPLA Director of Government Affairs**

In my previous column in this newsletter, I addressed global regulatory and legislative issues covering the European Union's General Data Privacy Regulation and California's Consumer Privacy Act, along with several measures being reintroduced in the current two-year 116th Congress. In this article I will comment further on the status of the 2017 Equifax consumer information breach in reference to proposed congressional action to combat future cybersecurity attacks. The Federal Trade Commission's role in protecting consumer privacy and data security will also be addressed. A survey of U.S. consumers conducted by the analytics company SAS Institute, Inc., indicates that 67 percent say the government should do more to protect their privacy. In the February 2019 issue of *Corporation Counsel*, Lisa Malloy, Intel Corporation's head of governmental affairs, states that if ever a time would come when a federal data privacy regulation would be passed, 2019 will be the year.

Congress is presently broken. Many investigative and security professionals are unaware of the unintended consequences of ill-conceived legislation that if not actively monitored and continually addressed, will adversely affect this profession. For over two decades, the federal legislative branch of our government has failed to enact a comprehensive data breach security bill; however, each of the 50 states has. There will be a strong lobbying effort that any federal bill that eventually passes both the House and Senate contain a preemption provision over states' laws regarding a uniform notification time of security breaches to affected parties.

It will be incumbent upon INTELLNET to take positive action as an association to ensure that no provisions of any anti-breach, artificial intelligence, or privacy legislation contain a provision defining private sector investigations as being synonymous with the business of information broker. Presently, the leadership in other national professional associations may not be effectively utilizing their resources to properly face the challenges we will be forced to deal with in the future. Will INTELLENET's leadership and its membership do so?

**“Presently, the leadership in other national professional associations may not be effectively utilizing their resources to properly face the challenges we will be forced to deal with in the future.**

**Will INTELLENET's leadership and its membership do so?”**

### Equifax Executives Believe They Did All They Could to Prevent Their Breach

A Congressional Senate Subcommittee interviewed current and former Equifax employees from its information security and IT departments relative to their massive 2017 security breach that reportedly affected a third of Americans. Their responses varied, but most said they believed that their security team’s actions were an appropriate response to the Apache Struts vulnerability. The Director of Global Threats and Vulnerability Management from 2014 to 2017 said “security wasn’t first” at

Equifax before the data breach, but that the data breach "made everyone focus on it more." The former Countermeasures Manager in place from 2016 to 2017 said he believed the response to the vulnerability was "not only defensible, but justifiable." The CIO at Equifax from 2010 to 2017 oversaw the company employees responsible for installing patches, but said he was never made aware of the Apache Struts vulnerability and did not understand why the vulnerability "was not caught." He did not think Equifax could have done anything differently. Federal lawmakers disagree.

***Equifax failed to properly preserve all documents including key internal chat records related to the breach.*** Several current and former Equifax employees stated that they regularly used an internal chat system, Microsoft Lync, to communicate with other Equifax employees throughout the company. These individuals told the Subcommittee they used Microsoft Lync to communicate real-time findings related to the breach once they discovered the suspicious activity. They also told the Subcommittee they used Lync to discuss subsequent response efforts. While the company's document retention policy defines a "record" to include any document written in the course of company business, Equifax considers these Lync types of chats to be disposable records. While the legal hold was issued on August 22, 2017, Equifax did not begin to preserve Lync chats until September 15, 2017. Therefore, the Subcommittee does not have a complete record of documents concerning the breach."

***TransUnion and Experian avoided a breach.*** TransUnion and Experian received the same information as the public and Equifax regarding the Apache Struts vulnerability, but the approach that each company took to cybersecurity was different from Equifax's. Both companies had deployed software to verify the installation of security patches, ran scans more frequently, and maintained an IT asset inventory. In response to the Apache Struts vulnerability, TransUnion began patching vulnerable versions of the software within days. Experian retained a software security firm in March 2017 to conduct targeted vulnerability scans of Apache Struts vulnerabilities. After finding an Experian server was running a vulnerable version, Experian took the server offline and began patching it. There is no indication that TransUnion or Experian were attacked by hackers seeking to exploit the Apache Struts vulnerability.

**"Equifax's largest competitors, TransUnion and Experian, quickly identified vulnerable versions of Apache Struts and proactively installed the patch."**

Equifax's largest competitors, TransUnion and Experian, quickly identified vulnerable versions of Apache Struts and proactively installed the patch. While all three major consumer reporting agencies ("CRAs") had similar policies on vulnerability scanning and patching, TransUnion and Experian had an accurate and updated IT asset inventory, which they used to identify and track applications and software across their entire network. This allowed TransUnion and Experian to identify which applications on their networks were using vulnerable versions of Apache Struts. Once they identified the vulnerable applications, each company took steps to patch the applications in an effort to prevent a data breach.

## Recommendations for Congress

**(1) Congress should pass legislation that establishes a national uniform standard requiring private entities that collect and store Personally Identifiable Information (PII) to take reasonable and appropriate steps to prevent cyberattacks and data breaches.** Several cybersecurity recommendations, including a widely known framework from NIST, already exist. However, the framework is not mandatory, and there is no federal law requiring private entities to take steps to protect PII.

**(2) Congress should pass legislation requiring private entities that suffer a data breach to notify affected consumers, law enforcement, and the appropriate federal regulatory agency without unreasonable delay.** There is no national uniform *standard* requiring a private entity to notify affected individuals in the event of a data breach. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring data breach notification laws. In the absence of a national standard, states have taken signifi-

cantly different approaches to notification standards with different triggers for notifications and different timelines for notifying individuals whose information has been stolen or improperly disclosed.

**(3) Congress should explore the need for additional federal efforts to share information with private companies about cybersecurity threats and disseminate cybersecurity best practices that IT asset owners can adopt.** Several federal agencies have released materials discussing information sharing for cyber threats. In addition, there are dozens of Information Sharing and Analysis Centers ("ISACs") and Information Sharing and Analysis Organizations across several industries, sectors, and regions in the United States. However, participation in an ISAC is voluntary, formal meetings are rare, and ISACs are funded by members.

**(4) Federal agencies with a role in ensuring private entities take steps to prevent cyberattacks and data breaches and protect PII should examine their authorities and report to Congress with any recommendations to improve the effectiveness of their efforts.**

**(5) Private entities should re-examine their data retention policies to ensure these policies properly preserve relevant documents in the event of a cyberattack.** An incomplete record regarding how an attack occurred, what the attacker damaged or stole, and how a company responded to the attack can hinder efforts by law enforcement to investigate and prosecute attackers and prevent policymakers and enforcement agencies from taking steps to prevent future incidents.

## The FTC & Protecting Consumer Privacy and Data Security

Since the enactment of the Fair Credit Reporting Act in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace. The Commission's primary source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices. Under Section 5 and other authorities granted by Congress, the Commission has aggressively pursued privacy and data security cases in many areas, including information brokers, children's privacy, financial privacy, health privacy, and the Internet of Things. To date, the FTC has brought more than 65 cases alleging that companies failed to implement reasonable data security safeguards, and more than 60 general privacy cases.

Federal Trade Commission members recently testified before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce about its "efforts to effectively protect consumers and promote competition, while anticipating and responding to changes in the marketplace." Testifying on behalf of the Commission, were FTC Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips, Rohit Chopra, Rebecca Kelly Slaughter, and Christine S. Wilson. In essence they stated that the FTC is "committed to using its resources efficiently to protect consumers and promote competition through law enforcement, policy and research, and consumer and business education." They indicated that FTC law enforcement actions have helped return more than $1.6 billion to consumers during fiscal year 2018. FTC regulators received a sympathetic understanding at the congressional hearing and will no doubt receive greater powers and funds to police privacy by way of increased fines against large aggregators of personal identifying information. Although not specifically mentioning Facebook, Commissioner Rohit Chopra indicated that for large companies fines are merely a "parking ticket. The FTC is aiming to increase sanctions against Facebook, including taking action against CEO Mark Zuckerberg personally to hold him in account for Facebook's failure to honor a 2011 agreement over past privacy lapses regarding its mass user base.

There is no national uniform standard requiring a private entity to notify affected individuals in the event of a data breach. Instead, all 50 states, the

District of Columbia, and several U.S. territories have enacted their own legislation requiring public disclosure of security breaches of PII. Some states require notification after any breach of non-encrypted personal information, while others require notification only if the breach is likely to cause "substantial harm" to individuals. Some states require companies to notify affected individuals within a set number of days, while others simply require private entities to provide notice "without unreasonable delay." This creates a patchwork of uncertainty for companies and consumers responding to data breaches. For example, Target, one of the largest retail chains in the United States, notified the public seven days after learning that it suffered a data breach. By contrast, Yahoo! suffered data breaches in 2013 and 2014, but did not disclose them until 2016 and 2017, respectively.

## WhatsApp calls have been used to inject Israeli spyware onto phones, allowing them to be monitored.

WhatsApp has confirmed the vulnerability of its app but did not name the perpetrator. However, the Financial Times named Israel-based cybersecurity company, NSO Group, for the incident. WhatsApp has already indicated the attack looks as though it was conducted by a private company that works with governments to deliver spyware, and a 'select number' of users were targeted." The claims could raise serious problems for WhatsApp's reputation, which has been built on the privacy and security of the end-to-end encryption in its very popular texting and voice calling application. NSO Group is best known for its reported, though not confirmed, role in assisting the FBI in opening the phone of the San Bernardino mass shooter after Apple fought an FBI request to do so.

"NSO's technology is licensed to au-

thorized government agencies for the sole purpose of fighting crime and terror. The company does not operate the system, and after a rigorous licensing and vetting process, intelligence and law enforcement determine how to use the technology to support their public safety missions," NSO Group said in a statement. The company emphasized that it does not use the hacking tools itself, and the tools are "solely operated by intelligence and law enforcement agencies."

"We investigate any credible allegations of misuse and if necessary, we take action, including shutting down the system," the company said, though it did not clarify whether the WhatsApp issue represented a "misuse" of its tools, but a person familiar with the company said only licensed government intelligence and law enforcement agencies use its tools for "specific terror or criminal threats or investigations."

## City of Baltimore Breached by Hacked Tool of NSA

Baltimore recently suffered a crippling cyber attack that shut down all of its computers. Victims of such attacks have paid millions of dollars in ransom. At some time prior to April 2017, the U.S. National Security Agency suffered a cyberattack resulting in the loss of its "EternalBlue," a hacking tool now used by digital extortionist. The tool was dumped on-line by a group known as the "Shadow Brokers" and subsequently acquired by China, Iran, North Korea and Russia. The NSA failed to alert U.S. citizens or companies of their loss of this tool. Thus, Microsoft, and other technology firms, could not adequately prepare security patches to thwart the malware attacks that have been launched by foreign extortionists against state and local governments, hospitals, large and small businesses, and individuals.

According to the New York Times, in 2017 North Korea utilized the hacking tool "WannaCry" to shut down the British healthcare system, the German railway system and 200,000 organizations worldwide. Subsequently, "NetPetya" was utilized by the Russians against Ukraine, as well as major corporations for ransom. The Chinese state organization "Emissary Panda" has recently been identified as the party that hacked into Middle East governments with "Eternal Blue."

Not only Baltimore has been victim of a ransom ware cyberattack; Dallas, New York and San Antonio are

just a few among many others that have been victims as well. Cyber extortion has cost victims hundreds of millions in ransom ware. The NSA viewed its "External Blue" as so valuable that after the breach of its tool it failed to warn those that might be vulnerable to its illegal use. Microsoft's Tom Burt, corporate vice president of consumer trust, in a quote to the Times stated, "These exploits are developed and kept secret by governments for the expressed purpose of using them as weapons or espionage tools. They're inherently dangerous. When someone takes that, they're not strapping a bomb to it. It's already a bomb."

Microsoft's president Brad Smith proposed the creation of a "Digital Geneva Convention" wherein governments would "pledge to report vulnerabilities to vendors, rather than keeping them secret to exploit espionage or attacks." In 2017, Microsoft, Google and Facebook joined fifty countries signing a proposal by French President Emmannuel Macron, the Paris Call for Trust and Security in Cyberspace-- to end "malicious cyber activities in peacetime." Absent as signatories were China, Iran, Israel, North Korea, Russia and the United States.

*Bruce can be reached at BruceHulme@yahoo.com*

♦♦♦

**Special Report**

# The Opioid Crisis in America

It is important to be knowledgeable about the opioid crisis and what we can do to help ourselves, our families, first responders, employers, communities and the FBI as needed.

## A National Epidemic

According to the National Institute on Drug Abuse (NIDA), every day, more than 130 people in the United States die after overdosing on opioids1. The misuse of and addiction to opioids— including prescription pain relievers, heroin, and synthetic opioids such as fentanyl—is a serious national crisis that affects public health as well as social and economic welfare.

The Centers for Disease Control and Prevention (CDC) estimates the total "economic burden" of prescription opioid misuse alone in the United States is $78.5 billion a year, including the costs of healthcare, lost productivity, addiction treatment, and criminal justice involvement.

Earlier this year, the InfraGard National Members Alliance, a FBI and private sector partnership, released a list of resources for its members, compiled from advisories from the federal government, the Centers for Disease Control and other resources.

## Resources

InfraGard selected the following resources as key information sources for employers, their employees and everyone who has to address this crisis:

*Continued on next page ...*

.....

### The President's Commission on Combating Drug Addiction and the Opioid Crisis

https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Final_Report_Draft_11-15- 2017.pdf - Federal funding and Programs, Opioid Addiction Prevention, Opioid Addiction Treatment, Overdose Reversal & Recovery, Research and Development.

### Surgeon General's Advisory on Naloxone and Opioid Overdose

https://surgeongeneral.gov/priorities/opioid-overdose-prevention/naloxone-advisory.html - History, epidemic, overdose-reversing drug naloxone, information for patients and public, information for prescribers, substance use disorder treatment providers and pharmacists and references.

### Centers for Disease Control and Prevention (CDC) Efforts to End the Opioid Epidemic

http://ww.cdc.gov/opioids/ - Empower consumers to make safe choices; partner with public safety; support providers, health systems and payers; build state, local, tribal capacity; and conduct surveillance and research.

### Using Naloxone to Reverse Opioid Overdose in the Workplace: Information for Employers and Workers

https://www.cdc.gov/niosh/docs/2019-101/pdfs/2019-101- 508.pdf?id=10.266/NIOSHPUB2019101 - Background, opioids and work, considering a workplace naloxone use program, establishing a program, references.

### Infographic: State-by-State Breakdown of Opioid Regulations

https://www.athenahealth.com/insight/infographic-opioid-regulations-state-by-state -How state-by-state laws vary around prescription pain management, how the regulations line up with opioid prescription rates, state-by-state, and how state opioid prescribing rates compare, policy by policy.

### Nine Ways to Fight the Opioid Epidemic in Your Community

https://icma.org/articles/article/9-ways-fight-opioid-crisis-your-community

1. Create community coalitions to work together across sectors.
2. Develop ordinances and places for safe drug disposal.
3. Establish drug diversion task forces.
4. Provide training for first responders.
5. Use drug courts to fight opioid addiction and trafficking.
6. Create referral programs through law enforcement agencies.
7. Disseminate information about state laws that encourage interventions.
8. Build awareness about their state's prescription drug monitoring program.
9. Host community neighborhood events to put tools into the hands of every community sector.

### Twelve Ways Opioid Addiction and Treatment Differ in Older Adults

https://health.usnews.com/health-care/patient-advice/articles/2017-09-01/12-ways-opioid- addiction-and-treatment-differ-in-older-adults

1. Addiction rises as the senior population grows.
2. Years of chronic pain add up.
3. Other substances complicate opioid addictions.
4. Health stakes are higher.
5. Drug-shaming is a problem.
6. Overdoses are rising, too.
7. Detox may take longer.
8. Shame prevents some seniors from seeking treatment.
9. Even among seniors, generational differences exist.
10. Age-tailored treatment helps.
11. Environment counts.
12. Seniors in treatment tend to thrive.

If you become aware of possible unlawful acts related to the opioid crisis, you are right to be concerned. If you SEE SOMETHING, please SAY SOMETHING in a timely manner to law enforcement, security and/or your supervisor, and give the authorities the chance to make a difference.

*This information will be updated annually and suggestions for changes can be sent to InfraGard.*

♦♦♦