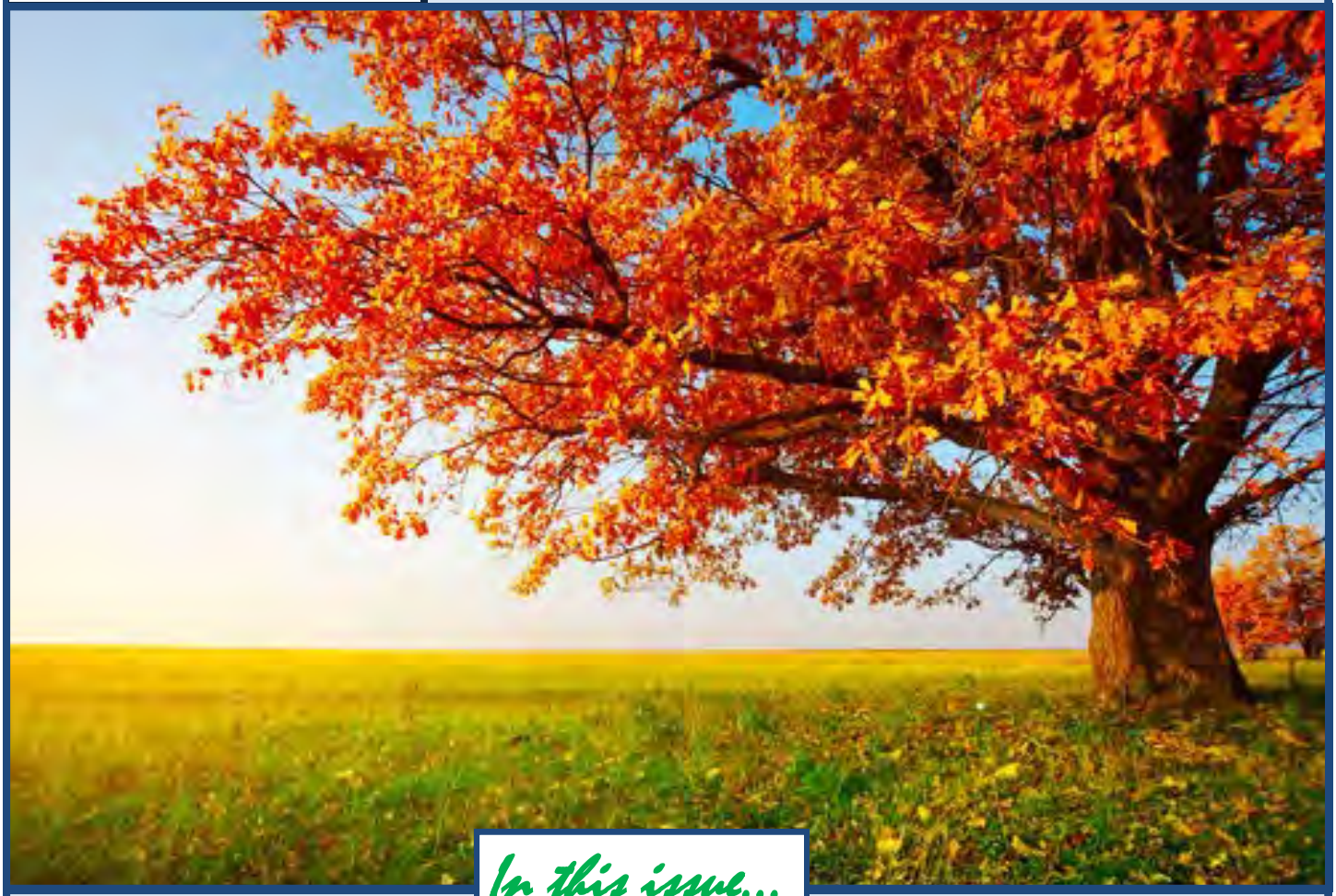
INTELLENET *News*

Official Newsletter of the
International Intelligence Network, Ltd.

Intellenetwork.org *Fall 2016*



In this issue...

Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet

Dear Intellenet Members:

As I sit here safe and sound in Michigan writing this piece …

My thoughts and prayers are with our members, their families, all the people in Florida and the rest of the region as hurricane Mathew hits. Times like these tend to bring up a lot of thinking about how to handle such events. My question to all of you is, do you have an emergency plan in place for your business? Whether your business is a one person operation or you have a lot of employees you need to have a plan in place. I'm not going to go into how you should implement an emergency plan for your business here, as there is plenty of good information on this subject that is readily available to all. I am sure there are members better qualified on this topic than I am who could write a great article for the benefit of all. That being said, I do encourage everyone to think about this important subject and be proactive. There are unlimited types of events that can turn into an emergency quickly and having a plan in place is going to give you better odds of your business surviving the event than having no plan at all.

We recently announced that our 2017 annual conference will be in Denver, Colorado April 20-22 with a pre-day training on April 19. Hotel reservations for our block of rooms is now open. I encourage everyone to make your reservations early instead of waiting to the last second. It is better to have room reservation and not need it later than not having a reservation and needing one at the last second. We are receiving an excellent rate of $129 (USD) per night. To make your reservations use the following link: http://www.intellenetwork.org/Annual-Conference.aspx.

George Michael Newman is hard at work putting together another exceptional lineup of speakers. He is also working on a very unique pre-day program that you will not want to miss, so make your travel plans accordingly. We are also planning on one or two additional outings during the conference. More information to come in the near future.

Intellenet exhibited at the World Investigators Conference over the summer in Texas and the LPDAM conference this fall. Many Intellenet members were speakers at both conferences. Both events were successful recruiting events for Intellenet. We will continue to do similar events around the country. We are seeing an upswing in retirements which we anticipate to increase in the next few years. It is important for Intellenet to continue to recruit new members throughout the world who qualify under our ten year experience requirement. As you network within your own business circles and attend conferences please keep a look out for qualified candidates. If you find someone you feel would be a qualified member please forward their contact information to me for follow up. Send the information to my email address peter@ewiassociates.com.

I wish everyone a great fall and winter season.

♦♦♦

Member News

Welcome New Members !

Tom BUCKLEY—Savannah, GA

Greg COOK —Huntington, WV

Jeff CROISETTE—Annapolis, MD

William GROSS—Spencer, WV

Dave JOHNSON—Corpus Christi, TX

Mike McHENRY—San Miguel de Allende, Mexico

Steve O'DANIEL—Nicholasville, KY

Bob WILKINSON—Gig Harbor, WA

These are our new members since we last published. Peter featured each in an InfoBrief. When you need "intel" in these locations, you now know where to turn. You can update your membership listings on the web and in the Briefcase Roster, by sending info to intellenet@intellenetwork.org.

Bill Blake featured on "PIs Declassified" ...

Intellenet member **William F. "Bill" Blake, CPP, CFE** was interviewed on the popular internet radio show, ***PIs Declassified***. Bill discussed the changing landscape for private investigators and the value of security consulting for expanding a PIs portfolio of offerings to clients. To hear the broadcast, click here. For more on the consulting workshop Bill references in the show, see page 5.

News from Apollo International ...

Longtime Intellenet member **Dennis M. Crowley Jr.,** one of our founding members from the ranks of the U.S. Air Force's OSI special agents and who served on our board for many years, notified us all on the listserve that he has sold his company, Apollo International, to Allied Universal. At the time of the sale, Apollo was the 12th largest security company in the U.S. Dennis' son, **Dennis Crowley III** (Denny), remains with Allied as an executive officer, and, of course, as an active Intellenet member.

Dennis and Peg Crowley at the Intellenet conference in Vancouver, May 16, 2012

Kevin McClain to speak at NALI's mid-winter conference in San Diego ...

On January 27, 2017 Intellenet member **Kevin McClain, CCDI** is scheduled to open the midwinter conference of the National Association of Legal Investigators at the Bahia Resort Hotel in the Mission Bay area of San Diego, California. Kevin will address a timely topic in his talk on investigating police misconduct. This will be an expanded version of his presentation before the National Association of Criminal Defense Lawyers. NALI's conference details will be posted soon on the web site, NALI.com. Intellenet member **George Michael Newman,** a longtime legal investigator who lives in San Diego, is sharing his program development talents with NALI, in addition to coordinating the Intellenet program for Denver.

♦♦♦

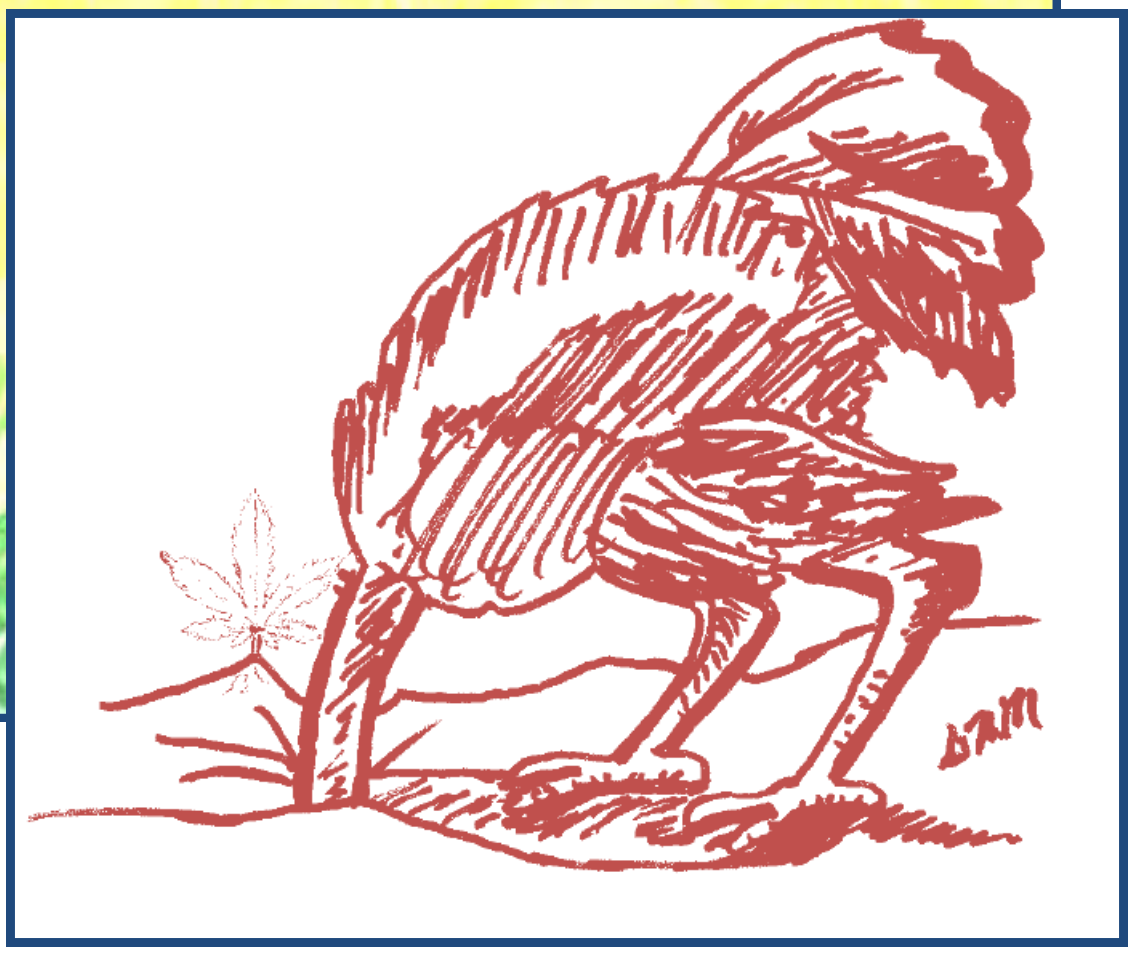
Intellenet Conference 2017

It just seems to abandon reason and logic to try and ignore inconvenient realities cresting the horizon.

Intellenet, rather than embracing an avoidance of impending social change, turns to face an on-coming tsunami during the 2017 annual conference in Denver, Colorado … one which investigators, in whatever capacity they may toil, most likely will inevitably encounter.

Stay attuned to upcoming announcements regarding the conference and the truly unique educational opportunity those in attendance are to be afforded.

George Michael Newman



Security Consulting Workshop

Intellenet has developed a security consulting workshop designed to assist the private investigator who wants to become a security consultant. The current active shooter and other hostile events have demonstrated that the small to medium size business owner normally does not have the staff or expertise to adequately protect their facility, their employees or business invitees. This program is designed to fill that void.

Increase Your Business Opportunities: Become a Security Consultant

This intensive, no frills workshop will be held at the CSI Academy of Florida, in Alachua, on January 12-13, 2017. The attendance fee is $129.00 and includes a continental breakfast and sandwich lunch each day. Attendees must make their own hotel reservations and the Best Western Gateway Grand Hotel has a $80.00 plus tax rate when the CSI Academy is mentioned. The following topics will be discussed:

What is Premises Liability and Negligent Security?—1 Hour

This presentation discusses the elements of the premises liability law and negligent security laws and possible risks areas.

What are the Risks to My Business?—2 Hours

This presentation will discuss the external and interna risks to a business and define the appropriate countermeasures to the identified risks.

Writing Your Risk Assessment Report—1 Hour

Writing a report to document the identified risks and appropriate countermeasures will be discussed to present the information in a professional manner.

Plaintiff/Defense Attorney Litigation Perspective—1 Hour with guest instructor

The opinions and comments on negligent security litigation will be discussed as identified by an attorney practitioner.

Developing Policies and Procedures—1 Hour

This presentation is a general discussion of writing security policies and procedures, including those procedures affecting all employees and those procedures restricted to designated departments.

Who are My Employees and Vendors?—1 Hour

This presentation will discuss conducting initial and periodic background investigations for employee and due diligence inquiries for vendors must be conducted in accordance with applicable laws.

Are the Physical Security Devices and Systems Adequate?—1 Hour

This presentation will discuss physical security devices and systems and their adequacy as long as they are employed in a manner to meet management expectations.

How Can I Market My Business?—1 Hour

This presentation will present a variety of business marketing strategies to assist in developing additional billable hours.

How Good is My Security Force?—1 Hour

This presentation discusses the selection, training and utilization of security personnel and appropriate security operational procedures.

Negligent Security Case Study—1 Hour

An actual negligent security litigation case will be discussed to identify the areas of negligence and how they could have been prevented.

How to Become a Security Expert Witness—1 Hour

An expert witness in security issues will be able to increase the number of billable hours and the billing rate for additional income.

Business Continuity Planning—2 Hours

The rate in which a business returns to complete operations following a disaster is the key to preventing financial disaster and bankruptcy.

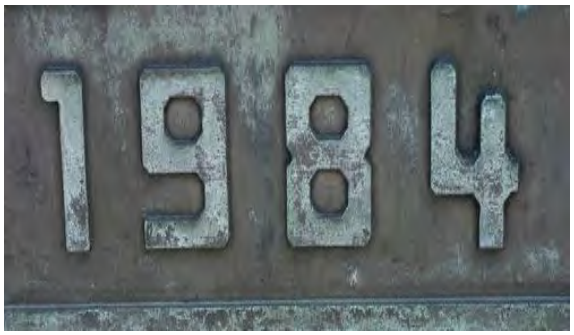
♦♦♦

Additional information, registration and fee payment are available at intellenetwork.org. Credit cards are acceptable.

How Modern-Day "Memory Holes" Undermine the Due Diligence Process

By Larry Gurwin, Senior Director – EMEA | Guidepost Solutions

Several years ago, a colleague and I conducted a background investigation of an English lord who was being considered for a senior position at an American company. His c.v. included directorships at several British companies but we soon discovered that he had "forgotten" a few companies, including one where he had served as non-executive chairman. Research on that company quickly revealed that it had gone bankrupt shortly after his tenure as chairman ended. Doubts about the candor of our subject prompted my colleague to nickname him "Lord Balderdash." Not surprisingly, he did not get the job.



The public records that revealed the gaps in the English lord's c.v. came from Companies House, the registry for companies formed in the United Kingdom. Companies House documents are an essential tool in due diligence investigations of companies and background checks on individuals -- which are really just a subcategory of due diligence.

Companies House's current policy is to retain records for 20 years but that may change. The registry is now considering a proposal to remove from the database the records of all companies that have been dissolved for more than six years.

This proposal has provoked widespread criticism from, among others, journalists, politicians, and activists. Roy Greenslade, a blogger for the *Guardian*, described the Companies House database as "indispensable for journalists, police officers, lawyers, researchers and bank compliance officials." One of the strongest objections came from *Private Eye*, a British magazine that combines satire with investigative journalism. The magazine noted that it relied on Companies House records in its reporting on BHS, a U.K. retail chain that recently collapsed in a major scandal. "Using such records last year," the magazine noted, "we revealed that BHS buyer Dominic Chappell had a history of business failures – companies dissolved between 1994 and 2005 that would not have been available in 2015 under the proposed new deletion regime."

When I learned about the proposal to delete old Companies House records, I immediately thought of *Nineteen Eighty-Four*, George Orwell's novel about a dystopian society ruled by the dictator Big Brother. One of the key techniques for manipulating the population is to rewrite history by feeding certain inconvenient documents and media reports into the "memory hole" -- a chute that leads to a giant incinerator.

The Companies House proposal is one of many modern-day examples of the "memory hole." Another is the so-called "right to be forgotten" which has caused Google and other search engines to delete thousands of links to media reports. This practice stems from a 2014 decision by the Court of Justice of the European Union in a case brought by a Spaniard named Mario Costeja González. Mr. Costeja was upset that Google searches of his name turned up a 1998 auction notice stating that his home had been repossessed. According to an EU Fact Sheet summarizing the case, he argued that the auction notice "infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these matters was entirely irrelevant."

In 2014, the Court ruled in Costeja's favor and began to require Google and other search engines to consider requests to remove certain links. This explains why a disclaimer often appears at the bottom of results pages warning that some results may have been removed. It's important to bear in mind that this so-called right is not absolute. In the words of the EU Fact Sheet, the court stated that : "**the right to be forgotten is not absolute**

but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (para 85 of the ruling). A **case-by-case assessment** is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role of the person requesting the deletion plays in public life might also be relevant."

It is also worth noting that while links are removed the underlying information usually remains. Google's (or Bing's) link to a newspaper article might vanish but the article itself will probably still be available in the newspaper's archives, in press databases, and – for the hopelessly analog – in hard-copy versions of the newspaper.

Why should we care about the modern-day memory holes? In cases like Mr. Costeja's, it may not matter very much. In other cases, the disappearance of information from the public domain can have serious consequences by omitting vital information from due diligence and KYC reports, creating a highly distorted picture of the subjects of the reports. Of course, on the positive side people like "Lord Balderdash" will undoubtedly be pleased.

♦♦♦

Larry Gurwin serves as senior director for Guidepost Solutions' Europe, Middle East and Africa (EMEA) practice. He has spent much of his recent time conducting and managing due diligence investigations and managing international asset searches. He can be contacted at lgurwin@guidepostsolutions.com.

Guidepost Insights

Intellenet Members Shine at the LPDAM Conference in September

ISPLA News for INTELLENET

by

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

As I write this report for INTELLENET, I am preparing for my, roughly, 20th conference and board meeting of the International Association of Security & Investigative Regulators. These meetings have been held at various locations throughout the United States and Canada. My sixth two-year term as IASIR's elected board member representing the private investigative profession will also come to a end.

2016 IASIR Conference
Turning Private Investigations and Security to the Terror Frequency:
How Regulators Can Calibrate Policies to Mitigate Exposures

IASIR is comprised of 48 regulatory agencies in the U.S., Canada, France and the United Arab Emirates, working closely with elected industry board members representing Contract Security, Private Investigation, Alarm, and Armored Car companies. In addition to these allied industry representatives, I've worked closely with the Armored Car Association, ASIS, Electronic Security Association, INTELLENET, ISPLA, NALI, NASCO, NCISS and many state professional associations. For more than two decades I have worked tirelessly to obtain IASIR board resolutions and help prepare IASIR testimony before Congress that is favorable to investigative and security professionals.

In recent years, some major issues I have brought before IASIR conferences and their board have included the "disrupter" Trustify unlicensed practice debate, state deregulation of private investigation and security, UAS (Drones) commercial use regulation by private investigators and for physical security purposes, social media investigations, GPS tracking, anti-pretexting, anti surreptitious surveillance, SSN redaction, public records closure legislation and regulatory, training and vetting issues of interest to state and provincial regulators.

The 2016 IASIR Conference will held in Las Vegas at the Golden Nugget October 26-28. Details for colleagues wishing to attend are at www.IASIR.org, or call their administrator, Laurel Rudd, at 888/354-2747. It is important to investigative and security professionals that IASIR continue to be supported by INTELLENET. I hope you will consider joining me there.

White House Report on Forensic Evidence ...

The President's Council of Advisors on Science and Technology's final report on forensics has concluded that much of the most common scientific analysis used in criminal trials does not meet scientific standards. It has raised questions about the use of bite-mark, hair, footwear, firearm and tool-mark analysis as evidence in thousands of trials annually in state and federal courts. Although it sets the stage for criminal-defense challenges of long-held evidentiary methods and promises increased courtroom battles with prosecutors over the use of expert witnesses, the Department of Justice has not accepted the

report's findings.

Forensic science, which has captured the imagination of the public in the 21st century with the popularization of TV shows like CSI, first came under widespread scrutiny in 2009, with a report by National Research Council entitled "Strengthening Forensic Science in the United States: A Path Forward." It called for major reforms to the criminal justice system-- and to establish national forensics scientific standards.

A White House panel of experts, including federal judges, are recommending that some forensic disciplines be thrown out of courtrooms, while some others need further scientific validation. The report blasts some analyses that have drawn recent scrutiny, including bite marks and hair follicles. But the report also contends that the culture needs to change to focus on fact-finding in the laboratory – and not on-the-job experience during criminal investigations.

"Casework is not scientifically valid research, and experience alone cannot establish scientific validity," the report states. "In particular, one cannot reliably estimate error rates from casework because one typically does not have independent knowledge of the 'ground truth' or 'right answer.'"

The group included nine federal judges, a former U.S. Solicitor General, a state supreme court justice, law school deans, and statisticians, concluded that forensic science results be "repeatable, reproducible and accurate."

The forensic review recommended:

- DNA mixtures. The combined-probability of inclusion (CPI) analysis of complex mixtures does not have a valid foundation, they found. Instead, probabilistic genotyping software needs to be further validated by third parties.

- Bitemarks and hair analysis, which have come under fire over the last year, do not meet scientific standards.
- Shoeprints and footwear comparisons, beyond size and make, are not scientifically valid.
- Latent fingerprints are "heading in the right direction" from a forensic science standpoint – especially with a recent FBI "black box" analysis.
- Firearms and ammunition comparison need to be better explained to juries. But a fully-automated analysis method could be coming in the near future, which would provide further validation.

The panel held a massive 2002 FBI study of the hair analysis as a "landmark of forensic science," due to its scientific standards. That study eventually led to reconsideration of tens of thousands of criminal convictions – but only after more than a decade had elapsed.

The group also recommended that the FBI Laboratory assume more of a lead role in the ongoing "overhaul" of the forensic science, through training, research, and validation of existing and future technologies. More government funding should be directed to agencies to further forensic scientific study, they added.

"The total level of federal funding by NIJ, NIST and NSF to the academic community for fundamental research in forensic science is extremely small," they write. "Substantially larger funding will be needed to develop a robust research community and to support the development and evaluation of promising new technologies."

The American Association for the Advancement of Science has undertaken what could become a "transformational" reevaluation of American forensic science, in response to the 2009 report. Ten disciplines are going to be subject to investigation. First up is ballistics and tool markers, latent fingerprints and arson investigations. Those are already underway.

The next seven are: bloodstain pattern analysis, digital evidence, footwear and tire tracks, bitemark analysis, fiber trace evidence, hair trace evidence, and trace evidence of paint and other coatings, according.

"Voodoo Science" Sending People to Prison ...

Many people languish in prison based on "voodoo science" that is presented as unassailable by forensic examiners, according to a

federal appeals judge.

Writing for the Wall Street Journal, Judge Alex Kozinski calls for amending federal law to allow federal courts to grant relief to prisoners who can show they were convicted based on false or overstated expert testimony. Currently the Antiterrorism and Effective Death Penalty Act "severely limits" the ability of federal courts to review state convictions, he says.

Kozinski served as a senior adviser to the report that finds flaws in forensic evidence and the way it is presented in court. The report from the President's Council of Advisors on Science and Technology "provides a road map for defense lawyers to challenge prosecution experts," he wrote. The report concluded that bite mark evidence "is about as reliable as astrology," Kozinski said. "Mumbo jumbo" that claimed char patterns indicate arson led to the execution of a Texas man. A fingerprint recovered from a Madrid train bombing was said to belong to an American lawyer—until authorities decided it was from another man.

The report's found that the effectiveness of mixtures of DNA from several people needs more testing. Fingerprint analysis can be subjective and affected by confirmation bias. The experts can't identify the source of bite marks with reasonable accuracy. A rigorous study of the error rate for firearm tracing found it could be as high as 1 in 46. Studies of worn footwear treads are lacking. The accuracy of hair analysis has been overstated.

The report recommends adopting standards to validate forensic methods, training forensic examiners, and making forensic labs independent of police and prosecutors. "All should be swiftly implemented," according to Judge Kozinski.

The FBI criticized the report, saying in a statement that it "makes broad, unsupported assertions regarding science and forensic science practice." Attorney General Loretta Lynch also issued a statement. "We remain confident that, when used properly, forensic science evidence helps juries identify the guilty and clear the innocent, and the department believes that the current legal standards regarding the admissibility of forensic evidence are based on sound science and sound legal reasoning," Lynch said.

Discovery Misconduct: SCOTUS To Hear $2.7M Sanction Case Against Attorneys …

The U.S. Supreme Court has accepted combined cases challenging a $2.7 million sanction for discovery misconduct imposed against Goodyear Tire & Rubber and two lawyers representing the tire maker.

The cases to be heard are *Goodyear Tire & Rubber Co. v. Haeger* and *Musnuff v. Haeger*. The two questions to be presented are:

1. In *Int'l Union v. Bagwell*, 512 U.S. 821 (1994), this Court ruled that sanctioned parties must be afforded the protections of criminal due process where sanctions are punitive, but not where they are compensatory. In this case, in a divided decision, the Ninth Circuit affirmed a $2.7 million sanction award imposed under inherent powers as a compensatory sanction. The majority held that sanctions can be compensatory even if the specific amount of sanctions is not directly caused by the alleged misconduct.

The first question presented is:

1) Is a federal court required to tailor compensatory civil sanctions imposed under inherent powers to harm directly caused by sanctionable misconduct when the court does not afford sanctioned parties the protections of criminal due process?

In *Roadway Express v. Piper*, 447 U.S. 752, 766 (1980) and *Chambers v. NASCO, Inc.*, 501 U.S. 32, 50 (1991), this Court held that a finding of subjective bad faith is required to award attorneys' fees as sanctions under inherent powers. In this context, the court of appeals held that a client is deemed bound by the acts of its attorneys and can suffer attorneys' fees as sanctions for its attorneys' alleged misconduct.

The second question presented is:

2) May a court award attorneys' fees under its inherent powers as sanctions against a client for actions by its attorney that are not fairly attributable to the client's own subjective bad faith?

The court agreed to decide the first issue where parties sanctioned under a court's inherent powers aren't given the protections of criminal due process, should the sanction be tailored to harm directly caused by the misconduct? A judge in Arizona had imposed the sanction for failure to disclose tire test results during discovery in a suit by two married couples who blamed the crash of their motor home on a failed tire. The case had settled in 2010, but the couples' attorney filed a motion for sanctions the next year

after reading an article about the testing. The federal judge sanctioned Fennemore Craig lawyer Graeme Hancock $550,000, and jointly sanctioned Goodyear and its national coordinating counsel Basil Musnuff $2.2 million. The sanction represented all of the attorney fees and costs incurred by the plaintiffs after Goodyear's first discovery responses.

The San Francisco-based 9th U.S. Circuit Court of Appeals upheld the sanction in July 2015. However, the dissenting judge, Paul Watford, had argued the sanction was punitive, which require protections available to criminal defendants, rather than compensatory, which requires only adequate notice and an opportunity to be heard. A sanction isn't compensatory, he argued, unless there is a causal connection between the alleged misconduct and the amount awarded.

EUROPOL Releases 2016 Internet Organised Crime Threat Assessment …

The 2016 Internet Organised Crime Threat Assessment (IOCTA), dated September 28, 2016, is the annual presentation of the cybercrime threat landscape released by Europol's European Cybercrime Centre (EC3). The 72-page 2016 report provides a predominantly law enforcement focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last year. It is based on valuable contributions by EU Member States and the expert input of Europol staff, which has been further enhanced and combined with input from our partners in private industry, the financial sector and academia. Many of the key threats remain largely unchanged from the previous report. Ransomware and banking Trojans remain top malware threats; a trend unlikely to change for the foreseeable future. While the same data stealing malware largely appears year-on-year, ransomware – a comparatively more recent threat – is in greater flux and may take several more years before it

reaches the same level of equilibrium. Peer-to-peer networks and the growing number of forums on the Darknet continue to facilitate the exchange of child sexual exploitation material (CSEM); while both self-generated indecent material (SGIM) and content derived from the growing phenomenon of live-distant child abuse, further contribute to the volume of CSEM available.

Cryptocurrencies, specifically Bitcoin, remain the currency of choice for much of cybercrime, whether it is used as payment for criminal services or for receiving payments from extortion victims. Even so, key members of the Bitcoin community, such as exchangers, are increasingly finding themselves the victim of cybercriminals. The growing misuse of legitimate anonymity and encryption services and tools for illegal purposes poses a serious impediment to detection, investigation and prosecution, thereby creating a high level of threat cutting across all crime areas. For law enforcement in particular, this creates a dichotomy of value. Strong encryption is highly important to e-commerce and other cyberspace activity, but adequate security depends on police having the ability to investigate criminal activity.

EMV (chip and PIN), geoblocking and other industry measures continue to erode card-present fraud within the EU, forcing criminals to migrate cash out operations to other regions. Logical and malware attacks directly against ATMs continue to evolve and proliferate. The proportion of card fraud attributed to card-not-present (CNP) transactions continues to grow, with e-commerce, airline tickets, car rentals and accommodation representing the industries hit hardest. The first indications that organized crime groups (OCGs) are starting to manipulate or compromise payments involving contactless (NFC) cards have also been seen.

The overall quality and authenticity of phishing campaigns has increased, with targeted (spear) phishing aimed at high value targets - including CEO fraud - reported as a key threat by law enforcement and the private sector alike. The assessment confirms that cybercrime remains a real and significant threat. It also highlights how those criminal techniques and methods which have traditionally been associated with cybercrime are extending into other crime and threat areas. A growing range of threats, from trafficking in human beings to terror-

ism, are becoming increasingly cyber-facilitated.

Other cross-cutting issues, such as the growing misuse of legitimate anonymity and encryption services and tools for illegal purposes pose a serious impediment to detection, investigation and prosecution of criminals. The report provides a number of key recommendations to address the issues and challenges outlined, and identifies several priority topics to inform the definition of operational actions for EU law enforcement in the framework of the EMPACT Policy Cycle.

These include clear actions under the three main mandated areas of the EC3 – cyber attacks, child sexual exploitation online, and payment fraud – such as: targeting criminals providing essential services and developing key tools which facilitate the activities of their criminal counterparts; eliminating communities which promote the production and sharing of child sexual exploitation material; and coordinated action to combat money mules.

Internet of Things (IoT) Implications: Future Threats and Developments …

The increasing amount of data that is being collected and processed via the IoT creates new privacy, cybersecurity and trust issues and risks. Because of the scale of the IoT, trust between different devices and across different platforms can be hard to engineer and expensive to guarantee. The decision support and contextual awareness offered by smart devices will make them and any supporting infrastructure a target for criminal data manipulation too.

It is inevitable that the new types of 'critical infrastructure' created by the IoT, as well as existing infrastructures, will be the targets of novel hybrid threats such as new forms of extortion involving hacked smart devices (ranging from very small medical devices, to smart cars, smart container

ships and smart cities), data theft, attacks resulting in physical and mental harm, and new types of botnets175. Such attack scenarios would not be limited to a particular category of attackers or a particular set of motives.

New approaches to increasing cybersecurity for the IoT and to establishing trust and ensuring privacy in the decentralized network it creates may include the use of the blockchain or Distributed Ledger Technology (DLT) 176. DLT can potentially provide a framework to facilitate transaction processing and coordination among interacting IoT devices. It may also be applied to ensure that the operating system and firmware used in a smart component of critical infrastructure has not been tampered with.

An area of particular concern is the field of biosecurity and the link to the increasing market of private companies offering DNA sequencing. Unlike stolen credit card information, someone's DNA fingerprint cannot be 'invalidated' once it has been leaked.

EU Legislative Implications ……..

Since the publication of the previous IOCTA, the European Union has not yet introduced a new legislative framework to harmonize the cybercrime legislation of the Member States. One topic closely related to cybercrime is cybersecurity. Focus was therefore on the drafting process of the EU Directive on Network and Information Security (NIS Directive). It was adopted in July 2016. While the Directive addresses various issues related to cybersecurity in general it does not contain any provisions specifically focusing on cybercrime. However, the Directive states that Member States should encourage operators of essential services to report incidents to law enforcement. In any case, the NIS Directive will impact the entire cyber security ecosystem and its implementation will likely require cooperation between the various stakeholders, including law enforcement and the judiciary.

A second initiative that is worth mentioning is the work of the Commission in the field of fraud related to non-cash payments. Currently the 2001 Framework Decision combating fraud and counterfeiting of non-cash means of payment is the main legal instrument. It contains a provision related to computer-related fraud – a typical cybercrime. The European Agenda on Security includes a review of this Framework Decision. The list of planned Commission initiatives consequently includes the proposal for a Directive combating Fraud and Counterfeiting of Non-Cash Means of Payment. The Roadmap published in May 2016 includes various references to Cybercrime and the challenges for

investigations due to the transnational dimension of offences such as "phishing" and "pharming". Furthermore, the data protection reform work done by the Commission has a direct impact on the effectiveness of criminal investigations into cybercrime. The reform package includes the General Data Protection Regulation (GDPR, adopted in April 2016) and the Data Protection Directive for the police and criminal justice sector (DPD, adopted in December 2015). The package will enhance the exchange of data between law enforcement authorities and harmonize data protection requirements across the EU.

Lastly, although strictly speaking not a legislative development, two sets of Conclusions, which have been adopted by the Council of the European Union under the Dutch Presidency, should be noted here. The first set of Conclusions regard the establishment of a European Judicial Cybercrime Network supported by Eurojust, where judicial authorities (prosecutors, judges and In some cases police officials) can meet and discuss developments and challenges in the fight against cybercrime, as well as exchange practical information and best practices. All with a view to facilitate and enhance cooperation between the competent judicial authorities. The second set of Council Conclusions is aimed at improving criminal justice in cyberspace and calls on the Commission to explore and where necessary develop a common EU approach for (1) cross-border access to electronic evidence for the purpose of criminal investigations, (2) cooperation between law enforcement authorities and cloud providers and (3) establishing jurisdiction in cyberspace.

The 2016 IOCTA sets priorities and helps to streamline resources within the EU and internationally to respond to cybercrime in an effective and concerted manner, supported by Europol. Despite the increasing challenges, the last 12 months have demonstrated that a coordinated approach by EU law enforcement that includes all relevant partners can result in significant successes in the fight against cybercrime, including in the important areas of prevention and awareness.

Police Officers Abuse Confidential Databases ...

A September 28, 2016 AP item reported out of Denver, CO, states police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work. Criminal-history and driver databases give officers critical information about people they encounter on the job. But the AP's review shows how those systems also can be exploited by officers who, motivated by romantic quarrels, personal conflicts or voyeuristic curiosity, sidestep policies and sometimes the law by snooping. In the most egregious cases, officers have used information to stalk or harass, or have tampered with or sold records they obtained.

No single agency tracks how often the abuse happens nationwide, and record-keeping inconsistencies make it impossible to know how many violations occur.

However, the AP, through records requests to state agencies and large major U.S. city police departments, found law enforcement officers and employees who misused databases were fired, suspended or resigned more than 325 times between 2013 and 2015. They received reprimands, counseling or lesser discipline in more than 250 instances, the review found.

Unspecified discipline was imposed in more than 90 instances reviewed by AP. In many other cases, it wasn't clear from the records if punishment was given at all. The number of violations was surely far higher since records provided were spotty at best, and many cases go unnoticed.

Among those punished: an Ohio officer who pleaded guilty to stalking an ex-girlfriend and who looked up information on her; a Michigan officer who used the system to obtain home addresses of women he found attractive; and two Miami-Dade officers who ran checks on a journalist after he aired unflattering stories about the department.

The databases searched included information on driver's licenses, vehicle registration information and criminal history. Officers searched the databases for information on romantic partners, business associates, neighbors, journalists, celebrities and politicians.

In some cases, police officers used the information to stalk people or to ask them for dates; to conduct criminal records checks for their own private businesses; and to investigate journal-

ists or politicians viewed as antagonistic to police departments.

"It's personal. It's your address. It's all your information, it's your Social Security number, it's everything about you," said Alexis Dekany, the Ohio woman whose ex-boyfriend, a former Akron officer, pleaded guilty last year to stalking her. "And when they use it for ill purposes to commit crimes against you - to stalk you, to follow you, to harass you ... it just becomes so dangerous."

The misuse represents only a tiny fraction of the millions of daily database queries run legitimately during traffic stops, criminal investigations and other police encounters. But the worst violations profoundly abuse systems that supply vital information on criminal suspects and law-abiding citizens alike. The unauthorized searches demonstrate how even old-fashioned policing tools are ripe for abuse, at a time when privacy concerns about law enforcement have focused mostly on more modern electronic technologies. And incomplete, inconsistent tracking of the problem frustrates efforts to document its pervasiveness.

The AP tally, based on records requested from 50 states and about three dozen of the nation's largest police departments, is unquestionably an undercount.

Some departments produced no records at all. Some states refused to disclose the information, said they don't comprehensively track misuse, or they produced records too incomplete or unclear to be counted. Florida reported hundreds of misuse cases of its driver database, but didn't say how often officers were disciplined.

And some cases go undetected, officials say, because there aren't clear red flags to automatically distinguish questionable searches from legitimate ones.

"If we know the officers in a particular agency have made 10,000 queries in a month, we just have no way to (know) they were for an inappropriate reason unless there's some consequence where someone might complain to us," said Carol Gibbs, database administrator with the Illinois State Police.

"If we know the officers in a particular agency have made 10,000 queries in a month, we just have no way to (know) they were for an inappropriate reason unless there's some consequence where someone might complain to us," said Carol Gibbs, database administrator with the Illinois State Police.

The AP's requests encompassed state and local databases and the FBI-administered National Crime and Information Center, a searchable clearinghouse that processes an average of 14 million daily transactions.

The NCIC catalogs information that officers enter on sex offenders, immigration violators, suspected gang members, people with outstanding warrants and individuals reported missing, among others. Police use the system to locate fugitives, identify missing people and determine if a motorist they've stopped is driving a stolen car or is wanted elsewhere.

Other statewide databases offer access to criminal histories and motor vehicle records, birth dates and photos.

Officers are instructed that those systems, which together contain data far more substantial than an internet search would yield, may be used only for legitimate law enforcement purposes. They're warned that their searches are subject to being audited and that unauthorized access could cost them their jobs or result in criminal charges.

Yet misuse persists —

"Sense of Being Vulnerable" ..

Violations frequently arise from romantic pursuits or domestic entanglements, including when a Denver officer became acquainted with a hospital employee during a sex-assault investigation, then searched out her phone number and called her at home. A Mancos, Colorado, marshal asked co-workers to run license plate checks for every white pickup truck they saw because his girlfriend was seeing a man who drove a white pickup, an investigative report shows.

In Florida, a Polk County sheriff's deputy investigating a battery complaint ran driver's license information of a woman he met and then messaged her unsolicited through Facebook, according to records.

Officers have sought information for purely personal purposes, including criminal records checks of co-workers at private businesses where they worked. A Phoenix officer ran searches on a neighbor during the course of a longstanding dispute, records show, and a North Olmsted, Ohio, officer

pleaded guilty this year to searching for a female friend's landlord and showing up in the middle of the night to demand the return of money he said was owed her.

The officer, Brian Bielozer, told the AP he legitimately sought the landlord's information as a safety precaution to determine if she had outstanding warrants or a weapons permit. But he promised as part of a plea agreement never to seek a job again in law enforcement. He said he entered the plea to avoid mounting legal fees.

Some database misuse occurred in the course of other misbehavior, including a Phoenix officer who gave a woman involved in a drug and gun-trafficking investigation details about stolen cars in exchange for arranging sexual encounters for him, according to records. She told an undercover detective about a department source who could "get any information on anybody," a disciplinary report says.

Eric Paull, the Akron police sergeant who pleaded guilty last year to stalking Dekany, also ran searches on her mother, men she'd been close with and students from a course he taught, prosecutors said. A lawyer for Paull, who was sentenced to prison, said Paull has accepted responsibility for his actions.

"A lot of people have complicated personal lives and very strong passions," said Jay Stanley, an American Civil Liberties Union privacy expert. "There's greed, there's lust, there's all the deadly sins. And often, accessing information is a way for people to act on those human emotions."

Other police employees searched for family members, sometimes at relatives' requests, to check what information was stored or to see if they were the subjects of warrants. Still other searchers were simply curious, including a Miami-Dade officer who admitted checking dozens of officers and celebrities including basketball star LeBron James.

Political motives occasionally surface, too .....

Deb Roschen, a former county commissioner in Minnesota, alleged in a 2013 lawsuit that law enforcement and government employees inappropriately ran repeated queries on her and other politicians over 10 years. The searches were in retaliation for questioning county spending and sheriff's programs, she contended.

She filed an open-records request that revealed her husband and daughter were also researched, sometimes at odd hours. But an appeals court rejected her suit and several similar cases this month, saying the plaintiffs failed to demonstrate the searches were unpermitted.

"Now there are people who do not like me that have all my private information ... any information that could be used against me. They could steal my identity, they could sell it to someone," Roschen said.

"The sense of being vulnerable," she added, "there's no fix to that."

Betrayal of Trust .....

Violations are committed by patrol officers, dispatchers, civilian employees, court personnel and high-ranking police officials. Some made dozens of improper searches, and some were under investigation for multiple infractions when they were punished, making it unclear whether database misuse was always the sole reason for discipline.

Agencies uncover some violations during audits, or during investigations into other misconduct. Some emerge after a citizen, often the target of a search, finds out or grows suspicious. A Jacksonville, Florida, sheriff's officer was found to have run queries on his ex-girlfriend and her new boyfriend after she raised concerns she was being harassed, an internal affairs report says.

The AP sought to focus on officers who improperly accessed information on others but also counted some cases in which officers divulged information to someone not authorized to receive it, or ran their own names for strictly personal purposes, including to check their car registrations.

The tally also includes some cases in which little is known about the offense because some agencies provided no details - only that they resulted in discipline.

The AP tried when possible to exclude benign violations, such as new employees who ran only their own names during training or system troubleshooting. But the variability in record-keeping made it impossible to weed out all such violations.

Agencies in California, for instance, reported more than 75 suspensions, resignations and terminations between 2013 and 2015 arising from misuse of the California Law Enforcement Telecommunications System, state records show. But because the records didn't identify officers or specify the allegations, it's unclear whether multiple violations were

committed by the same person or how egregious the infractions were.

Colorado disclosed about 35 misuse violations without specifying punishment. Indiana listed about a dozen cases of abuse but revealed nothing about them. The Florida Department of Highway Safety and Motor Vehicles reported roughly 400 violations in 2014 and 2015 of its Driver and Vehicle Information Database, or DAVID, but didn't include the allegations or punishment.

The FBI's Criminal Justice Information Services Division offers training to state and local law enforcement agencies on NCIC use, and conducts audits every three years that include a sample of local departments, said spokesman Stephen Fischer. But it doesn't track how often NCIC information is misused. Violations, which are not required to be reported directly to the FBI, are inconsistently disclosed to the federal government. The FBI relies on local agencies to address violations that are identified, Fischer said.

The AP requested records from large police departments and state agencies tasked with administering NCIC usage within their districts. The responses included cases where officers misused motor vehicle data, including driver's license and registration information, and also more sensitive criminal history records.

Officers only occasionally prosecuted, and rarely at the federal level.....

One recent exception is a former Cumming, Georgia, officer charged in June with accepting a bribe to search a woman's license plate number to see if she was an undercover officer. Another involved Ronald Buell, 49, a retired New York Police Department sergeant who received probation for selling NCIC information to a private investigator for defense attorneys.

At his July sentencing, Buell said he hoped other officers would learn "to never put themselves in the position I'm in."

Another (case) involved Ronald Buell, 49, a retired New York Police Department sergeant who received probation for selling NCIC information to a private investigator for defense attorneys.

Although prosecutions are rare, Buell, was sentenced to probation for selling the information, before his retirement, to a private investigator for defense lawyers. He could have faced up to five years in prison.

The case against the defendant Buell shed light on the role played by some retired officers in New York who work as private investigators and help defense lawyers investigate their clients' cases. The United States attorney's office for the Southern District of New York said that Buell deposited at least 17 checks, totaling nearly $9,000, that were issued by a private investigative firm run. In Federal District Court in Manhattan Buell told the judge, Alison J. Nathan, that around 2012 and 2013, he "agreed with a private investigator to search for certain information" from criminal justice databases "that only could be accessed" by authorized police personnel. He said he had "shared the results of the searches" with the investigator to assist him in his private cases and accepted checks as a "reward or gratuity for providing him the confidential police reports."

In one case cited in a criminal complaint, which signed by FBI Special Agent Peter Kilpatrick, the private investigator interviewed two eyewitnesses whose personal identifying information had appeared only in confidential police reports and had not yet been disclosed by the government to the defense. The investigation showed that a database inquiry relating to one of the witnesses had been made under Mr. Buell's password, the complaint said.

It's unsettled whether improper database access is necessarily a federal crime and whether it violates a trespass statute that criminalizes using a computer for other than authorized purposes. A federal appeals court last year reversed the computer-crime conviction of ex-NYPD officer Gilberto Valle, whom tabloids dubbed the "cannibal cop" for his online exchanges about kidnapping and eating women and who improperly used a police database to gather information. Valle argued that as an officer, he was legally authorized to access the database. The court deemed the statute ambiguous, and said it risked criminalizing a broad array of computer use.

Misuse occasionally prompts federal lawsuits under a statute meant to protect driver's license data.....

A Florida Highway Trooper, Donna Watts, accused dozens of officers of searching her in the state's driver database after she stopped a Miami officer for speeding in 2011. She al-

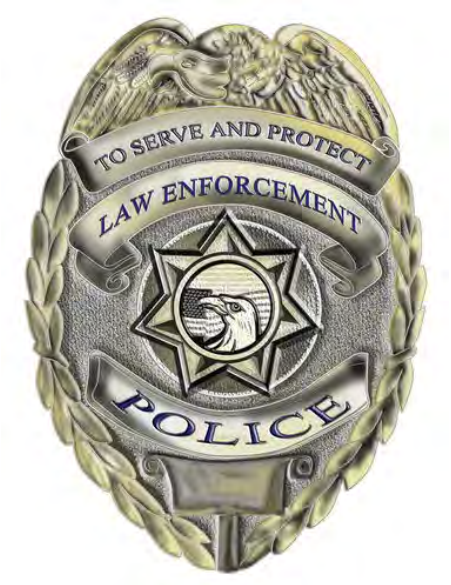
leged in lawsuits that she was harassed with prank calls, threatening posts on law enforcement websites and unfamiliar cars that idled near her home. Each unlawful access, she said in a court document, "has either caused or worsened anxiety, depression, insomnia, and other medical/physical/psychological conditions I suffer."

Law enforcement officials have taken steps to try to limit abuse, though they say they know of no foolproof safeguard given the volume of inquiries and the need for officers to have information at their fingertips. "There's no system that could prohibit you from looking up your ex-wife's new boyfriend, because your ex-wife's new boyfriend could come in contact with the criminal justice system," said Peggy Bell, executive director of the Delaware Criminal Justice Information System.

The Minnesota Department of Public Safety said it changed the way officers access a state driver database after a 2013 legislative audit found over half of the 11,000 law enforcement personnel who use it made searches that appeared questionable. The audit was conducted after a former state employee was charged with illegally viewing thousands of driver's license records.

In Florida, a memorandum of understanding this year increased the amount of field audits law enforcement agencies must undergo regarding DAVID usage. Troopers in the Florida Highway Patrol sign usage warnings when they access the DAVID system and a criminal sanctions acknowledgment. Users are subjected to audits and directed to specify a reason for a particular search before making inquiries.

Denver's independent monitor, Nicholas Mitchell, argued for strong policies and strict discipline as a safeguard, especially as increasing amounts of information are added to databases.



His review found most of the 25 Denver officers punished for misusing databases over 10 years received at most reprimands.

Miami-Dade police cracked down after the Watts scandal and other high-profile cases. The department now does quarterly audits in which officers can be randomly asked to explain searches. A sergeant's duties have been expanded to include daily reviews of proper usage and troubleshooting, said Maj. Christopher Carothers of the professional compliance bureau.

Even if the public is unaware of the amount of available information, Carothers said, "The idea that police would betray that trust out of curious entertainment or truly bad intent, that's very disturbing and unsettling."

ISPLA would like to add to this article that the first lawsuit for a violation of the federal Drivers Privacy Protection Act of 1994 was successfully prosecuted against a police officer and the municipality for which he was employed, by a plaintiff who was a private investigator in New York. The police officer had accessed the New York State DMV through a police database and provided personally identifiable information about the investigator and his family to two criminals the private investigator had under surveillance who were involved in a fraudulent workers compensation case against a food market chain.

Much of the information related in the above report came from reporters Eric Tucker in Washington, DC, Tom Hays in New York and AP video journalist Joshua Replogle in Akron, Ohio. ISPLA is grateful to The Pew Charitable Trusts (“Pew”) www.pewtrusts.org for providing us with much of this report.

"The Washington Post Takes Heat for Snowden's Prosecution Call" ...

A September 21, 2016 article in Security Week comments on the recent Washington Post editorial arguing for the prosecution of intelligence leaker Edward Snowden has sparked an outcry in the media community -- including from some of the newspaper's own journalists.

The controversial editorial provoked a heated response, with some pointing out the irony that the newspaper was calling for criminal charges against a source who helped it win a 2014 Pulitzer Prize for public service reporting. The editorial board "has no say on news, and just showed why,"

said a tweet from Barton Gellman, the Post reporter who led the team that shared the Pulitzer with The Guardian for the reporting on global surveillance based on Snowden's leaks of National Security Agency documents. Gellman added that Snowden's "disclosures served the public. WAPO journalists are proud of our role."

Jane Kirtley, a professor of media ethics and law at the University of Minnesota, said the Post's editorial view comes as a shock to the media community even if there is a separation of the opinion and reporting units.

"It does seem to me that any news organization that is going to rely on a source and potentially imperil that source, really needs to stand by that source," Kirtley told AFP. "I personally think Snowden should come back and face charges, but I didn't take Snowden's leaks and put them all over my newspaper," Kirtley stated, noting that prosecuting sources for leaks should be troubling for the world of journalism. "It is my belief that going after sources for leaks using the Espionage Act is a prelude to going after the journalists who receive that information," she said. "It hasn't happened yet, but it is possible."

Washington Post media columnist Margaret Sullivan also broke with the editorial board, calling for Snowden to be pardoned.

"Snowden did an important -- and brave -- service for the American public," Sullivan wrote in a column Tuesday. "Without his decision to bring the information to journalists, it is very unlikely that we would know what we do about mass surveillance in the post-9/11 world."

'Ignominious feat' .....

A more blunt response came from Glenn Greenwald, a member of the Guardian team that met with Snowden and now an editor at the online news site The Intercept.

"... Snowden also leaked details of basically defensible international intelligence operations" and "disrupted lawful intelligence-gathering, causing possibly 'tremendous damage' to national security."

"The Washington Post has achieved an ignominious feat in US media history: the first-ever paper to explicitly editorialize for the criminal prosecution of its own source -- one on whose back the paper won and eagerly accepted a Pulitzer Prize for Public Service," Greenwald wrote.

The debate comes amid increasing calls for a pardon for Snowden, who has been living in Moscow out of the reach of US law enforcement. The Post editorial argued that not only should Snowden not be pardoned, but that he should return to face charges and argue his defense "before a jury of his peers." The editorial acknowledged that Snowden justifiably exposed violations of law by the National Security Agency which helped lead to reforms.

But it added that Snowden also "leaked details of basically defensible international intelligence operations" and "disrupted lawful intelligence-gathering, causing possibly 'tremendous damage' to national security."

However, Fortune magazine media writer Matthew Ingram said it was troubling to see the comments from the Post, which has a tradition of investigative journalism which dates back to leaks in the Watergate scandal and Pentagon Papers case.

"Attacking and undermining the source that helped the company win a Pulitzer Prize looks hypocritical at best and craven at worst, and is almost certain to make future Snowdens think twice or even three times about going to the newspaper with a leak or a classified tip," Ingram wrote.

♦♦♦

Bruce Hulme, CFE, BAI is ISPLA's Director of Government Affairs. More at ISPLA.org