Jared,

On the heels of Wi-Fiber's **BEST OF SHOW award at CES**, our revolutionary **Intelli-Platform™** has garnered the attention of law enforcement offices as a **rapid Force Multiplier** at a fraction the expense of new officer hires and deployment! Police Departments across the country have become advocates of our approach and technology due to its nimble and open-source architecture. Our device, a straight replacement to traditional street lamps, incorporates **4K surveillance and high speed wireless connectivity**, which includes:

- Gunshot and glass-break sensors – Instant alerts with location accuracy
- 4K cameras with facial recognition & LPR – identification of perpetrators within minutes
- 911 hotline Two way speakers & PA System – Multiple communication methods
- Energy efficient dual LED Lamp with flash and color-change ability
- 4G network with wireless mesh Internet and Wi-fi connectivity

Modular design allows quick & easy maintenance and upgrades

Description: cid:intelli-platform.jpg

Best of all, with built-in wireless connectivity, power is the only requirement. The **Intelli-Platform** can be installed on any street corner with no additional internet or power lines. In the **City Las Vegas,** the devices were even mounted to a park wall, delivering connectivity, surveillance, illumination, and IoT functionalities, while CIO Michael Sherwood also successfully tested Bosch weather sensors, an Emergency Call Box, and multiple smart-city visualization suites - all powered by our device!

Do you have a few moments to discuss how our core capabilities can ensure safer, smarter and more connected streets and neighborhoods in the most cost effective Force Multiplier available?

Eric Burgdorf
Wi-Fiber
917.208.9538
wi-fiber.us

If you have trouble viewing this email, read the online version.

+

Reduce time-intensive, manual analysis of images and video

Analytics Desktop enables you to correlate, analyze and cross reference large amounts of media data quickly.

- Detect critical images and videos related to the investigation automatically using categories, such as weapons, faces, etc
- Identify persons of interest quickly with automatic facial recognition and advanced categorization
- Pinpoint the most relevant digital evidence

Learn more about media analytics, watch the video.

To get even more out of your trial, check out the tutorial:

Watch Tutorial

Visit us at www.cellebrite.com

Jared,

On the heels of Wi-Fiber's BEST OF SHOW award at CES, our revolutionary Intelli-Platform™ has garnered the attention of law enforcement offices as a rapid **Force Multiplier** at a fraction of the price of additional new hires. Our device, a straight replacement to traditional street lamps, incorporates high speed wireless connectivity and surveillance which includes:

- 4K cameras with facial recognition & LPR
- Microphones
- Two way speakers
- Gunshot and glass-break sensors

Best of all, with built in wireless connectivity, power is the only requirement - allowing your team to install our device on any and every street corner with no additional internet or power lines.

Do you have a few moments to discuss our core capabilities and the most cost effective force multiplier available?

Thanks & regards
Chris Maurer
Wi-Fiber LLC
Email: cmaurer@wi-fiber.us
Phone: 703-539-2490

Description:
https://c1.staticflickr.com/5/4732/27675676669_a9c3d0d072_n.jpg

PoliceOne.com

Police Products > Police Facial Recognition

Police surveillance technology under fire in appeal

A Florida court will determine whether police are allowed to use facial recognition software to identify suspects without ever notifying them of the technology

By Ben Conarck
The Florida Times-Union, Jacksonville

JACKSONVILLE, Fla. — The First District Court of Appeals is due to break new legal ground in determining whether police are allowed to use facial recognition software to identify suspects without ever notifying them of the technology.

The court battle, regarded by researchers as the first of its kind in the country to consider how the surveillance tool can be used in a criminal case, is being waged over a statewide biometric database of faces run out of the Pinellas County Sheriff's Office — one that extends to anyone with a Florida driver's license despite their criminal histories, or lack thereof.

Undercover detectives from the Jacksonville Sheriff's Office accessed the system through an intermediary in September 2015 to generate a lead after hitting a dead end in their search for the perpetrator of a $50 crack buy. More than two years later, state prosecutors with the Florida Attorney General's office are making novel arguments to defend the agency's use of the controversial technology.

The arguments are in response to Willie Allen Lynch's appeal of his May 2016 conviction for the sale of cocaine. The appellate judges will consider the case on numerous grounds — chief among them: whether the state was required to turn over photos of other matches returned by the face-matching software, and whether the subsequent identification process met legal standards.

The first issue centers on so-called "Brady material," named after a Supreme Court case that established the requirement that prosecutors turn over any evidence that might exonerate the defendant.

Lynch's attorneys are making the case that photos of four other potential suspects produced by the biometric database as potential matches would meet that definition. Lynch even requested those photos prior to trial after finding out they existed only by virtue of deposing detectives and a crime analyst months into the case.

Prosecutors hadn't proactively disclosed the way Lynch was identified by detectives, and his arrest report further obscured that identification, saying police used a mugshot system, which was only partially accurate. The mugshot system was linked to the facial recognition software.

THE BRADY CLAIM

The state's argument that prosecutors were not required to turn over the photographs even when asked centers on the fact that the undercover detective who identified Lynch considered only one of them — presented to him by a Jacksonville Sheriff's Office crime analyst, Celbricah Tenah.

"The trial court reasonably concluded that the evidence was not exculpatory because the undercover detectives only relied upon the single photograph sent by Tenah to identify the drug seller," prosecutors wrote in their brief.

The Lynch case was tried under former State Attorney Angela Corey. The current state attorney, Melissa Nelson, recently said her office has not set up policies directing line attorneys on how to manage facial recognition identifications in criminal cases because the issue doesn't come up often enough.

The Jacksonville Sheriff's Office also does not have a policy explicitly dealing with facial recognition. Lt. Chris Brown, of the Professional Oversight Unit, said the agency treats the technology as an investigative tool to generate leads, and its utilization falls under other policies and state law.

But privacy advocates and researchers who study the technology worry about a lack of specific safeguards to prevent misuse of the powerful technology .

In the Lynch case, the state's argument asserts that the other photos "played no role" in the detectives' identification of Lynch as the suspect.

"Moreover, there is no evidence that Tenah expressed doubt in the result of her search based on the other photographs," the brief said.

Lynch's lawyers argued that the trial court never held a hearing to determine whether the evidence was, in fact, exculpatory, despite Lynch requesting them, and that the photos would have been vital to their client's defense.

"Evidence that there were other men who fit the same facial profile as [Lynch] would have been significant in [Lynch's] attack on his identification as the seller," Lynch's attorneys wrote.

The state's failure to disclose them, they said, prejudiced Lynch's ability to defend himself against the charge and denied him due process.

"The error was not harmless and undermines confidence in the verdict," the lawyers wrote.

'UNDULY SUGGESTIVE'

Remarkably, despite having no legal training, Lynch, a lifelong addict, crafted legal arguments behind bars contending that the way detectives identified him — based on a single photograph presented by a crime analyst — was overly suggestive.

Typically, double-blind lineup procedures and other safeguards are used in the identification of suspects in criminal cases to prevent witnesses from being influenced by detectives, inadvertently or otherwise.

In Lynch's appeal, state prosecutors have conceded that "a single photograph of a suspect shown to a witness is generally considered highly suggestive," but contended that the case was outweighed by "the totality of the circumstances," namely that the detectives provided Tenah with three photos of the suspect taken during the drug deal.

"The three photos of the suspect at the drug transaction, [Lynch's] presence in the courtroom, and the photograph of [Lynch] from his arrest established mitigated the risk of misidentification by the detectives," prosecutors wrote.

Lynch's lawyers said that even beyond the "highly suggestive" procedure of Tenah showing the detective only the photo of Lynch, the crime analyst also told the detectives she thought Lynch was the drug seller and provided his criminal history, which included drug sales.

"If a police officer showed a single photo of a suspect to an eyewitness, told the eyewitness that he thought his suspect was the one who committed the crime, and told the eyewitness that the suspect in the photo had a history of committing the same kinds of crimes, then this court, or any court, would be hard-pressed to find there was not a substantial likelihood of misidentification," the defense attorneys wrote.

"The process used in the instant case was the functional equivalent."

'RED FLAG'

Clare Garvie, one of the country's foremost researchers in police surveillance technology, said that the state's contention that the other photos were not exculpatory is a "huge red flag," highlighting the frontier nature of the legal landscape being argued.

Further, Garvie added that the argument that the identification process was not unduly suggestive because the detectives were certain Lynch was the suspect "makes no sense."

Tenah, the crime analyst, played a central role in identifying Lynch, Garvie said, even though she was not a witness to the crime and was relying on algorithmic software she did not fully understand.

"This is just one example of the deeply concerning implications of the use of face recognition in law enforcement investigations," Garvie said.

Facial recognition software has come under fire by academic researchers such as Garvie for being mysterious in several regards. Accuracy has been called into question, as have methods and safeguards to make sure the systems work properly.

Other researchers have said the software has built in racial biases. Lynch is an African American male.

The court case has been ongoing and will stretch longer still. Prosecutors filed their response to the appeal in September, and the defense countered it two months later. The case is now awaiting a decision, which could still take several months.

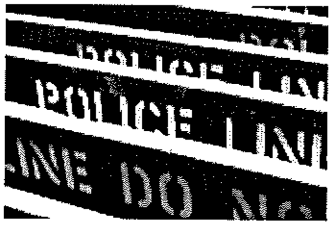
McClatchy-Tribune News Service

Tags > Investigations • Legal • Patrol Issues • Police Technology

Having trouble viewing this email? View it in your browser.

LexisNexis® RISK SOLUTIONS | Law Enforcement Webinar Series

Register for the February 28th human trafficking webinar for tips to find victims and stop criminals

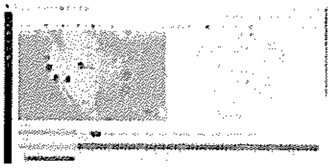


Human Trafficking: Tools and Methods for Successful Cyber Investigations

February 28 at 2:00 pm EST

The Internet has changed how human traffickers operate, enabling them to advertise their victims easily, anonymously, and to a large audience of buyers through various dating and relationship sites and various classified advertising platforms. This webinar, produced in partnership between Marinus Analytics and LexisNexis Risk Solutions, will show the best tools and methods to make use of this huge amount of data to find victims and traffickers successfully. It will cover how the data from LexisNexis law enforcement solutions like Accurint Virtual Crime Center in conjunction with Traffic Jam's artificial intelligence tools such as facial recognition through FaceSearch, can help rescue victims and complete searches in seconds. Join this webinar to gain tips and tools to make the most out of your time, to effectively find victims of human trafficking and bring their exploiters to justice.

Register Today



Introduction the Accurint Virtual Crime Center by LexisNexis

March 29 at 3:00 pm EST

Law enforcement experts will introduce how Accurint Virtual Crime Center is the next generation solution for investigations and nationwide data sharing. This solution helps your agency to solve more crimes and discover hard to find information by linking 10,000 public records sources to national law enforcement data to find non-obvious connections and generate leads with one search.

Register Today

Webinar Schedule

Apr 25, 2018 2:00 PM EST	Introducing the Accurint Virtual Crime Center by LexisNexis
May 23, 2018 1:00 PM EST	Making Connections: Linking Crimes at Local, Regional, and National Levels
Jun 26, 2018 2:00 PM EST	Introducing the Accurint Virtual Crime Center by LexisNexis
Jul 26, 2018 1:00 PM EST	Introducing the Accurint Virtual Crime Center by LexisNexis
Sep 26, 2018 3:00 pm	Introducing the Accurint Virtual Crime Center by LexisNexis

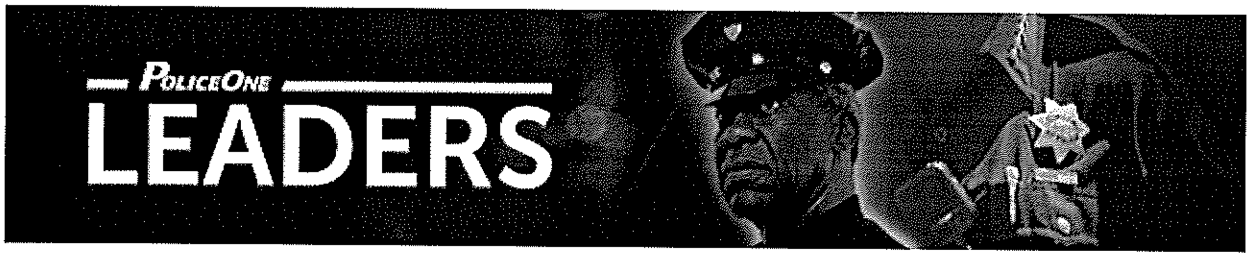
For more information on Accurint Virtural Crime Center, please click here.

Quick Links

Contact the Team
Product Training

Product Page

January 4, 2018 | View as webpage



Download the Mobile App

Dear Police Leader Member,

From body-worn cameras to bystander recordings, there's arguably nothing that's having a bigger impact on law enforcement than the rise of video technologies. As a police leader, you are responsible for determining how to best optimize these technologically-driven tools to keep both your cops and communities safe.

PoliceOne's latest digital edition, 2018 Police Video Guide: The emerging tech, training and tactics shaping law enforcement, is the definitive resource to guide your strategic implementation of video into day-to-day operations.

Download it here.

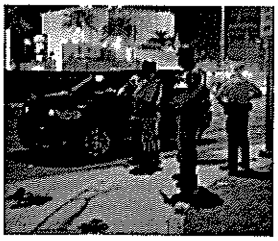
— *The PoliceOne Team*

FEATURED ARTICLE

How citizen surveys improve community engagement with police

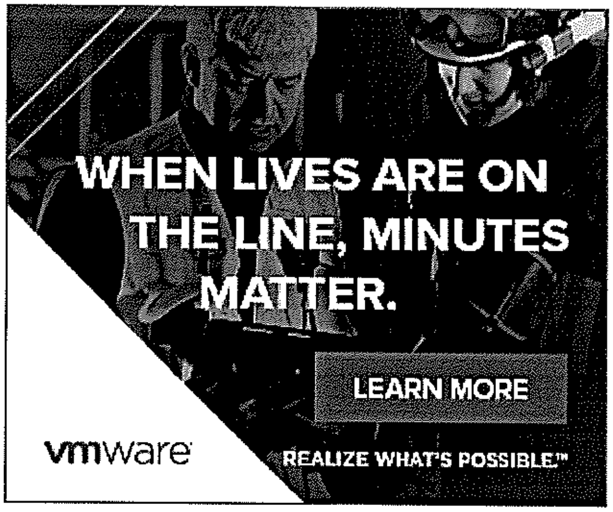
Citizen involvement >

Lessons in Leadership: Why cops shouldn't judge a crisis by its cover

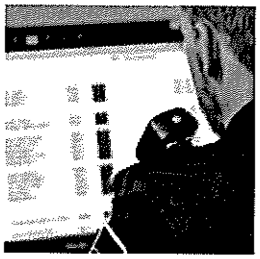


18 on 2018: Expert predictions on the top police issues in 2018

MORE POLICE LEADER COLUMNS >



White Paper: Improve the Public Safety Scheduling Process Through Automation

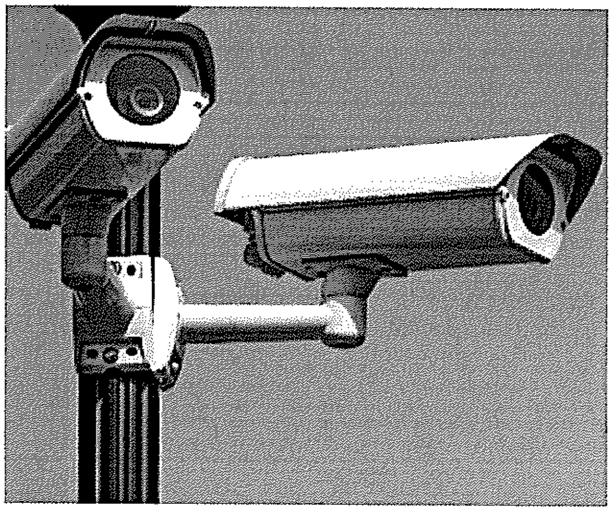


Download this free white paper to learn how an automated scheduling solution can improve fairness, achieve compliance, increase productivity, and reduce costs and financial risk.

Download this white paper

POLICING IN THE VIDEO AGE

How AI could monitor real-time camera feeds to detect criminal behavior



By Doug Wyllie, P1 Sr. Contributor

Using AI and facial recognition software for real-time crime reporting is the next progression in how police are using existing technology.

Logical progression >

POLICE TRAINING

How police agencies are training LEOs on the use of body cameras

By PoliceOne Staff

It's important to consider the level of training required to ensure successful use of the devices.

Biggest challenges >

View this email as a web page

SANS NewsBites

Annotated News Update from the Leader in Information Security Training, Certification and Research

December 18, 2018 Vol. 20, Num. 099

2018 NetWars Military Service Cup Results: The Air Force beat the Army (last year's winner) and Navy teams and Marines and Coast Guard as well in this year's Service Cup competition held in Washington DC. Lt. Gen. Edward Cardon presented the awards.

Top of The News

- Russian Disinformation Operations
- US Ballistic Missile Defense System Audit Finds Cybersecurity Problems
- GCHQ Officials Suggest How to Circumvent the End-to-End Encryption Problem

The Rest of the Week's News

- Updated Shamoon Infected Computers at Three Organizations
- Signal Says It Cannot Include a Backdoor in its App
- Facial Recognition Technology Used at Taylor Swift Concert in May
- Crowdstrike's Cyber Intrusion Services Casebook 2018: One Compromised Laptop Gave Hackers Access to Corporate Network
- Cloudflare Allegedly Counts Identified Terrorist Groups Among Clients
- Facebook Photos Exposed to App Developers
- Facebook Privacy Pop-Up Kiosk

Internet Storm Center Tech Corner

Cybersecurity Training Update

SANS Security East 2019 | New Orleans, LA | February 2-9

SANS Sonoma 2019 | January 14-19

SANS Miami 2019 | January 21-26

Cyber Threat Intelligence Summit & Training 2019 | Arlington, VA | January 21-28

SANS Las Vegas 2019 | January 28-February 2

SANS Northern VA-Tysons Spring 2019 | February 11-16

SANS Anaheim 2019 | February 11-16

SANS Dallas 2019 | February 18-23

Open-Source Intelligence Summit & Training 2019 | Alexandria, VA | February 25-March 3

SANS Amsterdam January 2019 | January 14-19

SANS Secure Japan 2019 | February 18-March 2

SANS OnDemand and vLive Training
Last Chance this year to Get a GIAC Certification Attempt Included or Take $350 Off with OnDemand or vLive. Offer Ends December 26.

Single Course Training
SANS Mentor and Community SANS

View the full SANS course catalog and skills roadmap

Free technical content sponsored by SANS

Top of the News

Report on Russian Disinformation Operations

(December 17, 2018)

A report commissioned by the US Senate Select Committee on Intelligence (SSCI) details analysis of the Russian Internet Research Agency (IRA) propaganda group's "influence operations targeting American citizens from 2014 through 2017." Among the report's key findings: there are "active and ongoing interference operations on several [social media] platforms"; there were "extensive operations targeting Black-American communities"; and the influence activity fomented "both secessionist and insurrectionist sentiments." The report was created by researchers from cybersecurity firm New Knowledge; Canfield Research, LLC; and the Tow Center for Digital Journalism at Columbia University.

Editor's Note

[Pescatore]
The Russian campaign focused on influencing the US presidential election, but the same tactics have and will be used in stock price manipulation and brand attacks. This is an area where marketing organizations are employing brand abuse monitoring services, fraud programs that take a different look, and email anti-phishing offerings that often include some overlap – good area for security teams to check around the company and work to integrate efforts.

Read more in:
- **www.wired.com**: How Russian Trolls Used Meme Warfare to Divide America
- **www.bbc.com**: Russia 'meddled in all big social media' in US election, says report
- **www.cyberscoop.com**: Russian disinformation ops were bigger than we thought
- **www.washingtonpost.com**: New report on Russian disinformation, prepared for the Senate, shows the operation's scale and sweep
- **disinformationreport.blob.core.windows.net**: The Tactics & Tropes of the Internet Research Agency (PDF)

US Ballistic Missile Defense System Audit Finds Cybersecurity Problems

(December 10, 14, 15, & 17, 2018)

According to a report from the US Department of Defense (DOD) Office of Inspector General (OIG), cyber protection for US ballistic missile defense systems (BMDS) lacks sufficient security. BMDS is designed to detect and intercept incoming missiles before they reach their targets. Nearly five years ago, the DOD CIO directed DOD to implement NIST security controls for systems protection. The report says that BMDS facilities have not fully implemented multi-factor authentication, do not consistently encrypt transmitted data, and that some known vulnerabilities remain unpatched. The facilities also failed to "protect and monitor classified data stored on removable media," and lacked intrusion detection capabilities on classified networks.

Read more in:
- **threatpost.com**: U.S. Ballistic Missile Defense System Rife with Security Holes
- **www.nextgov.com**: Poor Security Could Leave U.S. Defenseless Against Missile Attacks
- **www.bleepingcomputer.com**: U.S. Ballistic Missile Defense Systems Fail Cybersecurity Audit
- **www.scmagazine.com**: DoD Inspector General finds multiple flaws in missile defense system cybersecurity
- **www.dodig.mil/reports.html**: Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information DODIG-2019-034

GCHQ Officials Suggest How to Circumvent the End-to-End Encryption Problem

(November 29 & 30, 2018)

In an essay titled "Principles for a More Informed Exceptional Access Debate," Technical Director of the National Cyber Security Centre Ian Levy and Technical Director for Cryptanalysis for GCHQ Crispin Robinson describe how they envision law enforcement might intercept communications protected by end-to-end encryption. Levy and Robinson suggest that law enforcement could be silently added to a chat or a call by a service provider. The authors maintain that their "solution seems to be no more intrusive than the virtual crocodile clips that... [are] authorize[d] today in traditional voice intercept solutions."

Read more in:
- **www.lawfareblog.com**: Principles for a More Informed Exceptional Access Debate
- **www.zdnet.com**: GCHQ details how law enforcement could be silently injected into communications
- **techcrunch.com**: GCHQ's not-so-smart idea to spy on encrypted messaging apps is branded "absolute madness"

The Rest of the Week's News

Updated Shamoon Infected Computers at Three Organizations

(December 17, 2018)

A new variant of the Shamoon data-wiping malware is being used against organizations in Saudi

Arabia and the United Arab Emirates (UAE). Shamoon first appeared in 2012 when it was used to destroy more than 30,000 PCs belonging to Saudi Aramco. The new variant includes a component that erases files before wiping the master boot record, which makes it nearly impossible to recover data from a successfully infected machine. Italian oil service firm Saipem has disclosed its experience with the new Shamoon; Symantec says that at least two other organizations have seen machines infected with it.

Editor's Note

[Murray]
Enterprise data must be stored on servers with "least privilege" as the access control strategy, not on the desktop with "read/write" as the default access control rule.

Read more in:
- **www.darkreading.com**: Disk-Wiping 'Shamoon' Malware Resurfaces With File-Erasing Malware in Tow
- **www.bleepingcomputer.com**: Shamoon Disk Wiper Returns with Second Sample Uncovered this Month
- **www.saipem.com**: Saipem: Update On The Cyber Attack Suffered

Signal Says It Cannot Include a Backdoor in its App

(December 13, 14, & 15, 2018)

In a December 13 blog post, Signal developer Joshua Lund expresses the organization's frustration with Australia's new Assistance and Access bill, noting that "attempting to roll back the clock on security improvements which have massively benefited Australia and the entire global community is a disappointing development." Lund says that the Signal cannot include a backdoor and that "the end-to-end encrypted contents of every message and voice/video call are protected by keys that are entirely inaccessible to us."

Read more in:
- **signal.org**: Setback in the outback
- **www.zdnet.com**: Signal: We can't include a backdoor in our app for the Australian government
- **motherboard.vice.com**: Encrypted Messaging App Signal Says It Won't Comply With Australia's New Backdoor Bill

Facial Recognition Technology Used at Taylor Swift Concert in May

(December 12, 13, & 15, 2018)

Taylor Swift's security team used facial recognition technology at a May 2018 Rose Bowl concert to identify known stalkers. The technology was embedded in a kiosk that was playing clips of Swift's rehearsals; as concert-goers looked into the screen, a camera looked back at them. The captured images of concert-goers' faces were sent to a command center to be cross-referenced against a database of known stalkers. It is not known if concertgoers were aware that the technology was in use. Use of facial recognition technology in public places at large events is gaining traction; the 2020 Summer Olympics in Tokyo plans to use the technology for staff and athlete security checks.

Read more in:
- **www.theregister.co.uk**: Taylor's gonna spy, spy, spy, spy, spy... fans can't shake cam off, shake cam off

- **www.cnet.com**: Taylor Swift reportedly used facial recognition tech to identify stalkers
- **www.rollingstone.com**: Why Taylor Swift Is Using Facial Recognition at Concerts

Crowdstrike's Cyber Intrusion Services Casebook 2018: One Compromised Laptop Gave Hackers Access to Corporate Network

(December 14, 2018)

According to Crowdstrike's Cyber Intrusion Services Casebook 2018, a single laptop used at a coffee shop was infiltrated and used to gain access to an unnamed company's entire corporate network. The laptop user visited the website of a partner organization through a phishing email. In this particular case, the hackers exploited a misconfiguration in the company's Active Directory implementation that granted unnecessary privileges. The security software that the affected company used detected threats only when the device was being used within the organization's network.

Read more in:
- **www.zdnet.com**: How one hacked laptop led to an entire network being compromised

Cloudflare Allegedly Counts Identified Terrorist Groups Among Clients

(December 14, 2018)

A Huffington Post report alleges that Cloudflare is providing cybersecurity services to seven groups that are under sanctions from the US Treasury Department; of those, six are identified as foreign terrorist groups by the US State Department.

Editor's Note

[Pescatore]
All service providers have to deal with the "know your customer" issue and all the various sanctions that home country law places on doing business with blacklisted nations and countries. At any given time, many large service providers have compliance issues – the key is how quickly they deal with known or reported violations.

Read more in:
- **www.huffingtonpost.com**: U.S. Tech Giant Cloudflare Provides Cybersecurity For At Least 7 Terror Groups
- **www.cnet.com**: Cloudflare customers reportedly include foreign terrorist groups under US sanctions
- **gizmodo.com**: Cloudflare Under Fire for Allegedly Providing DDoS Protection for Terrorist Websites

Facebook Photos Exposed to App Developers

(December 14, 2018)

On Friday, December 14, Facebook acknowledged yet another data privacy mistake: for a two-week period in September 2018, more than 850 third-party app developers had access to photos belonging to 6.8 million Facebook users, regardless of the permissions users had granted. Facebook says the data leak problem was fixed in September 25.

Editor's Note

[Northcutt]
I do not believe there ever was, or ever will be, such a thing as a "private" photo posted to social medial, no matter what the platform.

Read more in:
- **www.wired.com**: Facebook Exposed 6.8 Million Users' Photos to Cap Off a Terrible 2018
- **www.theregister.co.uk**: Stop us if you've heard this one: Facebook apologizes for bug leaking private photos
- **www.zdnet.com**: Facebook bug exposed private photos of 6.8 million users
- **arstechnica.com**: "We're sorry," Facebook says, again—new photo bug affects millions
- **www.cyberscoop.com**: Facebook bug gave developers access to private photos of 6.8 million users

Facebook Privacy Pop-Up Kiosk

(December 12 & 13, 2018)

Last week, at the end of a year filled with data privacy troubles, Facebook set up a kiosk at a holiday market in New York City that was staffed with employees ready to answer people's questions about privacy, advertisements, and the company's data collection practices. Facebook is making a concerted effort to be clear that they are not in the business of selling users' personal data. A New York Times Op-Ed piece says that assertion is semantic skullduggery, observing that Facebook's practice of making sure advertisers' ads are shown to their desired target audience is tantamount to selling user data.

Editor's Note

[Neely]
Privacy controls can be confusing. Kudos to Facebook to spread understanding; users need to remember the slippery slope of expecting online information to remain private.

[Murray]
There are two kinds of Facebook users: the knowledgeable and the naive. Neither expects privacy from Facebook.

Read more in:
- **www.wired.com**: At a New York Privacy Pop-Up, Facebook Sells Itself
- **www.nytimes.com**: Congress May Have Fallen for Facebook's Trap, but You Don't Have To

Internet Storm Center Tech Corner

Magellan SQLite Vulnerability
https://blade.tencent.com

Logitech Options Vulnerability
https://bugs.chromium.org

Intel NUC BIOS Protection Flaw
https://embedi.org

Password Protected ZIP with Maldoc
https://isc.sans.edu

Memes Used as Covert Command and Control Channel
https://blog.trendmicro.com/

Shamoon Disk Wiper Malware is Back
https://unit42.paloaltonetworks.com

HiddenTear Ransomware Decrypter
https://www.bleepingcomputer.com

The Editorial Board of SANS NewsBites

SANS Institute
11200 Rockville Pike, Suite 200, North Bethesda, MD, 20852

PoliceOne.com

Topics > Policing in the Video Age > Articles

Cop Gumbo

with Val Van Brocklin

As commercial use of facial recognition expands, what are the implications for police?

If citizens willingly permit widespread use of FRT outside of law enforcement, you could argue they no longer have any reasonable expectation of facial privacy

Editor's Note:

Few forces are impacting law enforcement like video. **Policing in the Video Age**, P1's yearlong special editorial focus on video in law enforcement, aims to address all facets of the topic with expanded analysis and reporting.

In the final installment of this four-part signature coverage effort, we take a look at the future of video in policing. Click here to learn more about the project.

Also be sure to check out our latest PoliceOne Digital Edition – **2018 Police Video Guide: The emerging tech, training and tactics shaping law enforcement** – in which we explore how departments can best utilize emerging video technologies to enhance police officer safety and improve operational efficiencies. Download the free guide here.

POLICING IN THE VIDEO AGE
What is the future of video in policing?
PoliceOne Signature

Facial recognition technology (FRT) is a software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours.

The Fourth Amendment protects people from warrantless government searches or seizures where they have a subjective expectation of privacy that is deemed reasonable by public norms. The reasonableness standard is decided on the totality of circumstances.

In this Friday, Nov. 3, 2017, file photo, an Apple employee demonstrates the facial recognition feature of the new iPhone X at the Apple Union Square store in San Francisco. (AP Photo/Eric Risberg, File)

This is why the expanding commercial use of FRT is interesting. If citizens willingly permit widespread use of FRT outside of law enforcement, an argument could be made that they no longer have any reasonable expectation of facial privacy.

EXPANDING COMMERCIAL USES OF FACIAL RECOGNITION SOFTWARE

In 2008, Lenovo released a line of laptops that allowed users to log on using their face instead of a password. Windows 10 does the same.

Facebook, Apple and Google use facial recognition to assist in "tagging" images – identifying someone in a photo by name.

Other online services that have used facial recognition include:

- Face recognition search engines;
- Stylecaster – a website that allows women to upload their image and try on different makeup, clothes, and hairstyles;
- Snapchat – An image messaging app that allows users to apply lenses to photos using FRT

In 2012, 20 percent of all smartphones shipped had facial recognition capability. It's estimated that by this year, 665 million smartphones and tablets will include facial recognition.

In 2015, China unveiled the first facial recognition ATM. Facial recognition has been incorporated into smart TVs by LG, Samsung and Panasonic. The TV set offers menus based on who's watching. The Nielsen company is exploring the use of smart TVs for measuring ratings and determining who's watching shows and ads.

In February 2016, MasterCard announced it would accept "selfies" in place of passwords for signing into accounts. Similarly, Amazon filed a patent in March 2016 for a program that will allow users to authorize purchases by taking selfies.

Retailers are increasingly using the technology not just to prevent loss by identifying shoplifters but to improve sales by tracking legitimate shoppers. The Atlanta-based ad agency Redpepper is testing their project -- Facedeals. Users grant Facedeals access to their Facebook; Facedeals then learns the user's face. The idea is that stores, bars and restaurants rigged with Facedeals cameras will "recognize" users who have opted into the program – and will text a customized coupon to the user's phone based on their social media activity.

PUSHBACK AGAINST FACIAL RECOGNITION USE IN THE COMMERCIAL SECTOR

In Orwell's dystopian novel, "1984," everyone knew they were being watched and recorded by "The Party." The leader of The Party was called "Big Brother." From that came a pop culture phrase -- "Big Brother is watching you." It was my generation's metaphor for government intrusion.

But in 2013, one of the pioneers of FRT, Joseph Atick, told 60 Minutes, "Big Brother is no longer big government; Big Brother is big business."

More recently, the movie "The Circle" based on Dave Eggers' book imagines an alarming reality where everyone's personal information is readily shared and available on the internet. The Circle (a thinly-veiled, fictitious Facebook, Amazon and Google combined) would eliminate the need for search warrants.

The FBI's amassing of 411.9 million facial images for its Next Generation Identification (NGI) program has garnered plenty of media attention, but that lags well behind Facebook's 1.65 billion users. Facebook has the largest biometric database in the world – "and it's all been formed by people voluntarily submitting pictures to Facebook and identifying who they belong to," says Amie Stepanovich, director of the domestic surveillance project at the Electronic Privacy Information Center in Washington, D.C.

Facebook has refused to answer questions about what it does with its facial recognition information. Social media companies rarely talk about their internal systems. But in 2012, Facebook bought Face.com, whose company's founders had published a paper titled "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition."

Like the FBI's NGI program, the commercial sector's use of FRT is getting pushback. In 2014, the U.S. Department of Commerce held talks about whether and how commercial FRT should be regulated. The negotiations included representatives from consumer-advocacy groups and the tech industry. User privacy groups, including Electronic Frontier Foundation and the Consumer Federation of America, walked out. The industry and its lobbyists, they said, wouldn't even admit that users might want to consent to facial-recognition software so it was no use participating in the talks.

Recently, the Illinois Biometric Information Privacy Act has become the basis of a number of lawsuits against tech giants Facebook, Google, Shutterfly and Snapchat, with consumers claiming their biometric information was handled illegally.

One of the most-watched suits is that of three Illinois plaintiffs against Facebook, alleging the tech giant's collection, storage and subsequent use of biometric information without informed consent invaded their privacy. That case is making its way toward trial – or a settlement.

In Europe and Canada, privacy advocates won a victory last year when Facebook launched its photo app, Moments, without facial recognition scanning.

Plenty of Americans still feel they have some privacy rights to their faces – at least from being identified without their consent by businesses or the government. I wonder what they'll do if Facebook refuses to back down and tells them they can always opt out of Facebook. I wonder what they'll do when TSA offers a quick pass based on facial recognition to those who voluntarily participate, or retailers offer them discounts based on FRT.

If law enforcement waits awhile, the norm may well be that citizens have dealt away their facial privacy rights.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags > Legal

PoliceOne.com

Police Products > Police Facial Recognition

Cop Gumbo

with Val Van Brocklin

What police departments should consider before implementing facial recognition software

Police agencies need to know how to vet the technology and its vendors

---

In Orwell's dystopian novel, "1984," every citizen knows they're being watched. There are telescreens everywhere recording them. According to "the Party," this surveillance is for the betterment of the state as a whole, and citizens who resist or disobey are labeled traitors and disappear. The leader of the Party goes by "Big Brother."

The classic novel was assigned college reading for me. "Big Brother" was part of my pop culture lexicon – a synonym for government abuse of power as it related to civil liberties, often through mass surveillance. Today, watching, cataloging and identifying citizens aren't science fiction.

HOW FACIAL RECOGNITION SOFTWARE WORKS

NIST computer scientist Ross Micheals demonstrates a NIST-developed system for studying the performance of facial recognition software programs. (Photo/Robert Rathe)

Facial recognition software aims to identify or authenticate individuals by comparing their face against a database of known faces and looking for a match.

First, a computer must find the face in the image. Then it creates a numeric representation of the face based on the facial features. Finally, this numeric "map" of the face in the image is compared to database images of identified faces, for example, a driver's license database. There are almost as many computer algorithms for this process as there are companies.

Facial recognition has become more sophisticated in recent years.

Three-dimensional (3-D) facial recognition uses 3-D sensors to capture information about the shape of a face. Three-dimensional data points from a face vastly improve the precision of face recognition. One advantage of 3-D face recognition is that it's not affected by changes in lighting. It can also identify a face from a range of viewing angles, including a profile.

In 2015, Facebook announced its algorithm could identify people in unclear images or images in which people were not looking directly at the camera. Recently, according to Facebook's AI department, it doesn't even need a face but can identify people through hairdos, postures, gestures and body types.

Facial recognition accuracy depends on the algorithm used. In 2010, the U.S National Institute of Standards and Technology (NIST) tested various facial recognition systems and found that the best algorithm correctly recognized 92 percent of unknown individuals from a database of 1.6 million criminal records.

Currently, systems can reach reliability of up to 99 percent, depending on the image. It's more reliable than recognition by humans. In 2014, a study of border control officers with specific education and training in facial recognition found that fraudulent photographs were accepted in 14 percent of cases.

PUBLIC DEBATE OVER THE USE OF FACIAL RECOGNITION

Two recent reports have shined a spotlight on concerns about the accuracy and reliability of facial recognition. Both have received media attention.

In May 2016, the Government Accountability Office (GAO) issued a report on the FBI's Next Generation Identification (NGI) program which is amassing multimodal biometric identifiers such as face-recognition-ready photos, iris scans, palm prints and voice data, and making that data available to other agencies at the state and federal levels. The report criticized the NGI for its lack of transparency, absence of reliability testing and invasion of privacy.

In October 2016, Georgetown Law's Center for Privacy and Technology published findings from a year-long investigation based on over 15,000 pages of records obtained from over 100 FOIA requests. The report set out to inform the public about how facial recognition is used and the policies that govern how police can use it. Information about the FBI's use of facial recognition had been known. This report tried to tackle the scale of local and state law enforcement involvement.

Concerns about the reliability and accuracy of facial recognition include:

- While companies marketing the technology claim accuracy rates higher than 95 percent, the algorithms used by police are not required to undergo public or independent testing to determine accuracy or check for bias before being deployed on everyday citizens.
- Accuracy rates are not equal across algorithms. According to NIST, algorithms developed in China, Japan and South Korea recognized East Asian faces far more readily than Caucasians. The reverse was true for algorithms developed in France, Germany and the United States.

Facial recognition systems are more likely either to misidentify or fail to identify African Americans, errors that could result in innocent citizens being marked as suspects in crimes. Little is being done to correct for the bias. One study co-authored by a senior FBI technologist found that Cognitec, whose algorithms are used by police in California, Maryland and Pennsylvania, consistently performed 5-to-10 percent worse on African Americans than on Caucasians. One algorithm, which failed to identify the right person in 1 out of 10 encounters with Caucasian subjects, failed nearly twice as often with African Americans.

- This bias is compounded by the disproportionate number of African Americans who are surveilled, stopped, booked and have mug shots taken by police. (This isn't to say the algorithms are intentionally "racist." Rather, they are flawed on racial lines, probably unintentionally during the algorithms' development. An algorithm flaw in Google's facial recognition tagged two African Americans as "gorillas.")

- Facial recognition software often provides a list of possible matches. Police departments largely rely on officers to decide whether a candidate photo matches one in the list. A recent study showed that, without specialized training, humans make the wrong decision about such a match half the time.

- Face recognition systems aren't audited for misuse. Of the 52 police agencies queried in the Georgetown Law study, only nine (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, the Michigan State Police, provided documentation showing their audit regime was actually functional.

HOW POLICE DEPARTMENTS SHOULD PLAN FOR THE USE OF FACIAL RECOGNITION

There are several steps police departments should take when using facial recognition software:

- Police agencies are well-placed to require that facial recognition software vendors submit to NIST's existing accuracy tests and any new tests that it develops. Require vendors to address their algorithms' race, age and gender bias with accuracy tests and performance results.

- Provide training for officers who will be deciding whether there is a match amongst a list of possible candidates provided by facial recognition software.

- Log and audit the use of agency facial recognition software.

- Be transparent with your community about your facial recognition software, the vendor, accuracy testing, logging and auditing procedures.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags > Command Staff - Chiefs / Sheriffs • Legal

Images not showing up? Click here

NCJTC National Criminal Justice Training Center of Fox Valley Technical College

Conference is 2 weeks away- Have you registered yet?

11th Annual National Conference on Responding to Missing and Unidentified Persons

Sheraton Atlanta Hotel | 165 Courtland St. NE | Atlanta GA
September 19 - 21, 2017

LEARN MORE

SCHEDULE

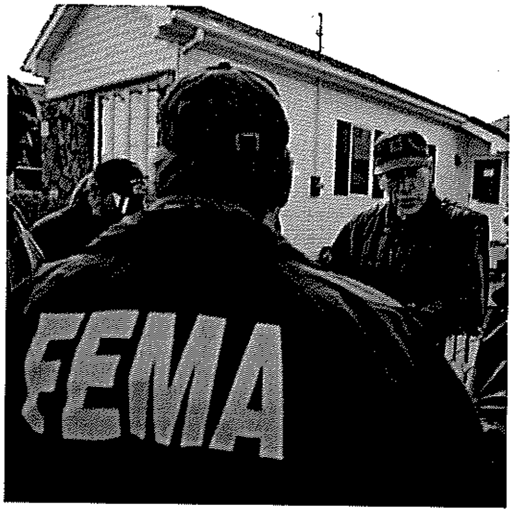
Georgia POST credits available

Three Training Focuses - Topics include:

Search and Recovery	• Case of Victoria Stafford Search • Missing and Murdered Native Women- the problem and response • Search for the Missing on Land, at Sea, and from the Air • Managing the Media in a Mass Casualty Event: Lessons learned from Sandy Hook
Investigation	• Benefits of Partnerships in Missing and Unidentified Persons Cases • Barway Collins Murder Case • Jacob Wetterling Investigation • Serial Predators and Human Trafficking
Resources	• Lessons learned from Katrina • Facial Recognition Technology • Canada's Missing Person DNA Program • Responding to International Parental Child Abductions

Spots still available for FEMA Course!

Emergency Operations Plans for Rural Jurisdictions



Certification Course- MGMT 383

September 21, 2017
Part 1 - 8:30 am - 12:00 pm
Part 2 - 1:30 pm - 5:00 pm

REGISTER

Still looking for lodging?

If you are still looking for accommodations at the Sheraton Atlanta Hotel, please contact Helen Connelly at dcoffice@fvtc.edu for assistance.

Questions? Please contact us at (888) 347- 5610 or email dcoffice@fvtc.edu

NCJTC
National Criminal Justice Training Center
Fox Valley Technical College

NATIONAL ASSOCIATION NASAR FOR SEARCH AND RESCUE

National Criminal Justice Training Center
(855) 866-2582 | info@ncjtc.org | ncjtc.org | facebook.com/ncjtc

Fox Valley Technical College
Knowledge That Works

NCJTC, 1825 N. Bluemound Drive, Appleton, WI 54914

SafeUnsubscribe™ jlavalle@northamptonma.gov
Forward this email | Update Profile | About our service provider
Sent by info@ncjtc.org

Images not showing up? Click here

Good Afternoon,

The Missing and Unidentified Persons Conference is happening in a few short months and I wanted to make sure that you were aware of the many topics that could enhance your agency's ability to carry out your responsibilities in these complex and difficult cases. .

In an effort to address the needs of law enforcement and search and recovery teams, we have developed three tracks of training:
1. Investigation
2. Search and Recovery
3. Resources.

We are also including a FEMA course on the final day of the conference for those looking to be certified in Emergency Plans Operations. We promise an informative must-attend event!

I invite you to review the information below and make plans to attend. Hope to see you in Atlanta this Fall.

Sincerely,

Bradley Russ
Director, National Criminal Justice Training Center of Fox Valley Technical College

NCJTC National Criminal Justice Training Center
of Fox Valley Technical College

Join us at the

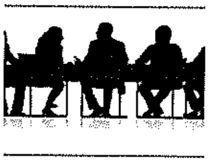
11th Annual National Conference on Responding to Missing and Unidentified Persons Conference

Multiple Victim Events: Implications for Investigation, Search, Rescue, and Recovery
September 19 - 21, 2017 | Atlanta, GA

Individual Registration $400	Groups of 3+ $350 per registrant
REGISTER	REGISTER

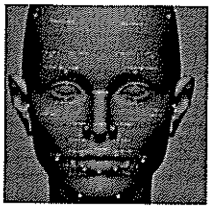
Plenary Sessions

Keynote Presentation:
Why Am I Here? Why Are You Here?
Amanda Pick, CEO, Missing Children Society of Canada



The Art of Possibilities
Panel of experts will discuss what's new in the field of missing persons cases, search and recovery, and technology.

Scratching the Surface: 27 years of Questions, Victimization, and Advocacy
Patty Wetterling, Parent | Jared Scheierl, Surviving victim
Jane Straub, Victim Advocate



Using Facial Recognition to Track Crime AND Find Missing Persons
Wyly Wade, President and CEO, Biometrica Systems, Inc.

Workshops

Investigation Track

Benefits of Partnerships in Missing and Unidentified Persons Cases
Barway Collins Case | Green River Killer | Serial Predators and Human Trafficking

Search and Recovery Track

Victoria Stafford Search | Managing the Media: Sandy Hook
Searching for Missing on Land, at Sea, and from the Air

Resources Track

NamUs | Lessons Learned from Katrina | Soil and Atmospheric Scent Dynamics

FEMA Certification and Field Resources Sessions

FEMA Emergency Operations Plans for Rural Jurisdictions,
Part 1 & 2 Certification Course MGMT383
Disappearance of Glenn Pennie | Diverse state and national resources
NCMEC Facial Reconstruction Expertise and Team Adam

Using NamUs & Sneak Peek at NamUs 2.0

Click more info for lodging, agenda and more details!

MORE INFO

Questions? Please contact us at (888) 347- 5610 or email dcoffice@fvtc.edu

NCJTC
National Criminal Justice Training Center
Fox Valley Technical College

NATIONAL ASSOCIATION NASAR FOR SEARCH AND RESCUE

National Criminal Justice Training Center
(855) 866-2582 | info@ncjtc.org | ncjtc.org | facebook.com/ncjtc

Fox Valley TECHNICAL COLLEGE Knowledge That Works

NCJTC, 1825 N. Bluemound Drive, Appleton, WI 54914

SafeUnsubscribe™ jlavalle@northamptonma.gov

Forward this email | Update Profile | About our service provider

Sent by info@ncjtc.org

Images not showing up? Click here

Good Afternoon,

The Missing and Unidentified Persons Conference is happening in a few short months and I wanted to make sure that you were aware of the many topics that could enhance your agency's ability to carry out your responsibilities in these complex and difficult cases. .

In an effort to address the needs of law enforcement and search and recovery teams, we have developed three tracks of training:
1. Investigation
2. Search and Recovery
3. Resources.

We are also including a FEMA course on the final day of the conference for those looking to be certified in Emergency Plans Operations. We promise an informative must-attend event!

I invite you to review the information below and make plans to attend. Hope to see you in Atlanta this Fall.

Sincerely,

Bradley Russ
Director, National Criminal Justice Training Center of Fox Valley Technical College

NCJTC National Criminal Justice Training Center
of Fox Valley Technical College

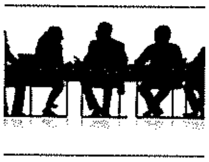
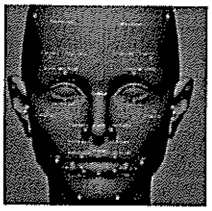
Join us at the

11th Annual National Conference on Responding to Missing and Unidentified Persons Conference

Multiple Victim Events: Implications for Investigation, Search, Rescue, and Recovery
September 19 - 21, 2017 | Atlanta, GA

Individual Registration $400	Groups of 3+ $350 per registrant
REGISTER	REGISTER

Plenary Sessions

	Keynote Presentation: Why Am I Here? Why Are You Here? Amanda Pick, CEO, Missing Children Society of Canada
	**The Art of Possibilities** Panel of experts will discuss what's new in the field of missing persons cases, search and recovery, and technology.
	Scratching the Surface: 27 years of Questions, Victimization, and Advocacy Patty Wetterling, Parent | Jared Scheierl, Surviving victim Jane Straub, Victim Advocate
	**Using Facial Recognition to Track Crime AND Find Missing Persons** Wyly Wade, President and CEO, Biometrica Systems, Inc.

Workshops

Investigation Track

Benefits of Partnerships in Missing and Unidentified Persons Cases
Barway Collins Case | Green River Killer | Serial Predators and Human Trafficking

Search and Recovery Track

Victoria Stafford Search | Managing the Media: Sandy Hook
Searching for Missing on Land, at Sea, and from the Air

Resources Track

NamUs | Lessons Learned from Katrina | Soil and Atmospheric Scent Dynamics

FEMA Certification and Field Resources Sessions

FEMA Emergency Operations Plans for Rural Jurisdictions,
Part 1 & 2 Certification Course MGMT383
Disappearance of Glenn Pennie | Diverse state and national resources
NCMEC Facial Reconstruction Expertise and Team Adam

Using NamUs & Sneak Peek at NamUs 2.0

Click more info for lodging, agenda and more details!

MORE INFO

Questions? Please contact us at (888) 347- 5610 or email dcoffice@fvtc.edu

NCJTC
National Criminal Justice Training Center
Fox Valley Technical College

National Association for Search and Rescue NASAR

National Criminal Justice Training Center
(855) 866-2582 | info@ncjtc.org | ncjtc.org | facebook.com/ncjtc

Fox Valley Technical College
Knowledge That Works

NCJTC, 1825 N. Bluemound Drive, Appleton, WI 54914

SafeUnsubscribe™ jlavalle@northamptonma.gov

Forward this email | Update Profile | About our service provider

Sent by info@ncjtc.org

Images not showing up? Click here

NCJTC National Criminal Justice Training Center *of* Fox Valley Technical College

Registration Open for 2017 Conference!

11th Annual National Conference on Responding to Missing and Unidentified Persons Conference

Multiple Victim Events: Implications for Investigation, Search, Rescue, and Recovery
September 19 - 21, 2017 | Atlanta, GA

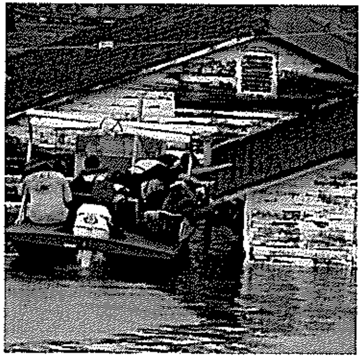
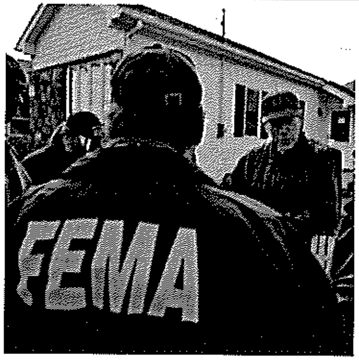
Individual Registration $400

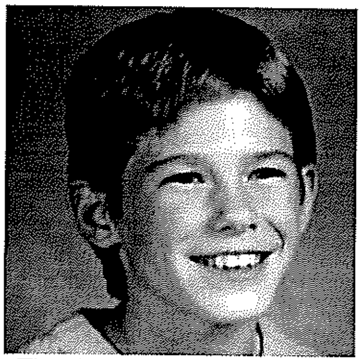
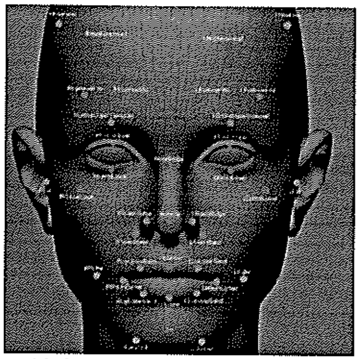
REGISTER

Groups of 3+ $350 per registrant

REGISTER

2017 Conference Highlights

Emergency Preparedness	FEMA Certification
	

Lessons Learned from Katrina	Emergency Ops Planning for Rural Jurisdictions
Panel Discussion	**Investigation Case Study**
 The Jacob Wetterling Story	Barway Collins
Public Information	**High Tech**
Managing the Media at Sandy Hook	 Using Facial Recognition Software

See our agenda for full details about the conference!

AGENDA

MORE INFO

Venue and Lodging

Sheraton Atlanta Hotel | 165 Courtland Street NE | Atlanta, GA
(404) 659-6500

MORE INFO

Questions? Please contact us at (888) 347- 5610 or email dcoffice@fvtc.edu

NCJTC
National Criminal Justice Training Center
Fox Valley Technical College

NATIONAL ASSOCIATION NASAR FOR SEARCH AND RESCUE

National Criminal Justice Training Center
(855) 866-2582 | info@ncjtc.org | ncjtc.org | facebook.com/ncjtc

Fox Valley TECHNICAL COLLEGE
Knowledge That Works

NCJTC, 1825 N. Bluemound Drive, Appleton, WI 54914

POLICEONE.COM

Cop Gumbo

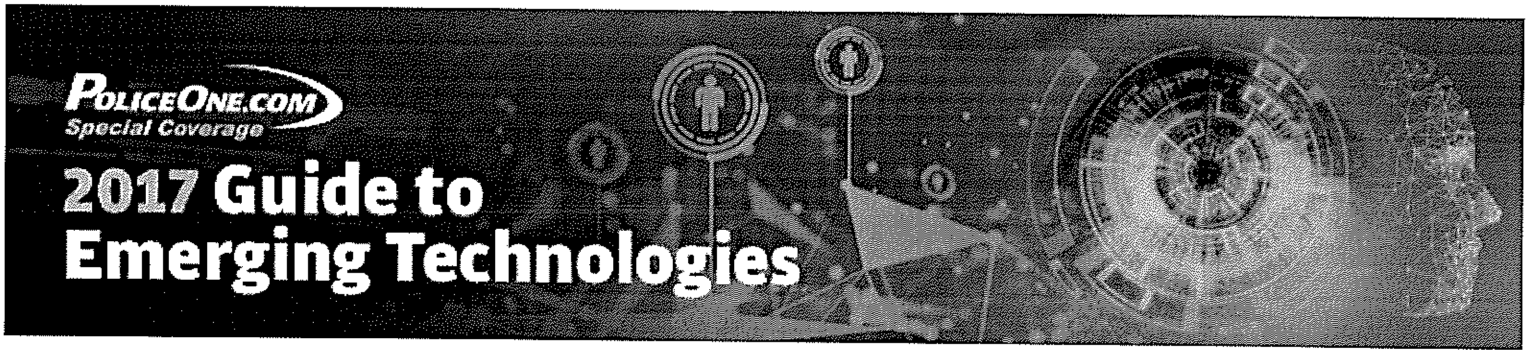
with Val Van Brocklin

Facial recognition technology and a 'reasonable expectation of privacy'

Law enforcement might consider using discretion before a court decides whether police need a warrant to scan someone's face

Editor's Note:

From crafting policy to tactical considerations, PoliceOne's **2017 Guide to Emerging Technologies** features expert analysis on soundwave technology, facial recognition software, handheld narcotics analyzers, the future of traffic stops, how constitutional law impacts the collection of data for investigations, and how advancements in biometric technologies will help improve correctional facilities.



Sept. 11 demonstrated that the greatest military might in the world couldn't protect us against the "asymmetric threats" of a few "unidentifiable enemies." The idea that FRT could identify terrorist suspects in public locations before they committed their crimes seemed to offer some protection.

Last May, the Government Accountability Office (GAO) issued a report about the FBI's amassing of 411.9 million facial images as part of its Next Generation Identification (NGI) program. It criticized the

programs secrecy and intrusion on privacy. Eighty percent of the photos were of people who had committed no crime. That's a significant police-created biometric database of primarily law-abiding Americans.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available.
(Photo/Pixabay)

"If you're reading this in the United States, there's a 50 percent chance that a photo of your face is in at least one database used in police facial-recognition systems," reported the Atlantic Monthly last October.

Georgetown Law's Center for Privacy and Technology published a report the same month addressing the scale of local and state police involvement in facial recognition. The year-long investigation was based on more than 15,000 pages of records obtained through more than 100 FOIA requests. It found that police departments in nearly half the states can use facial-recognition software to compare surveillance images with databases of ID photos or mugshots. Some departments only use the technology to confirm the identity of a suspect who's been detained; others continuously analyze footage from surveillance cameras.

The GAO and Georgetown Law's reports are fueling public debate, which often lags behind evolving technology – as do court decisions. To date, I could find no court ruling on police use of FRT and the Fourth Amendment's reasonable expectation of privacy against government intrusion absent probable cause and a warrant.

PUBLIC DEBATE

Proponents of police use of FRT argue:

- There is no expectation of privacy to your face once you take it out in public.

- Any privacy intrusion is a small price to pay for increased public safety.

- What difference does it make if the government has a digital algorithm of your face they can use to ID you if you haven't done – or aren't doing – anything wrong?

Privacy advocates' concerns include:

- A reasonable expectation of privacy includes a reasonable expectation of anonymity from government use of computer algorithms and databases to capture law abiding citizens' faces and identify them without their knowledge or consent.

- FRT allows for a different kind of tracking that can occur from far away, in secret, and on large numbers of people. Fingerprints are only left on things you touch and you know when police are taking them. You can't leave your face at home and, with limited exceptions, it isn't acceptable to cover it. Depending how it's used, FRT could rob citizens of a reasonable expectation of anonymity.

Giving police the rights to do this without judicial oversight creates a slippery slope that could lead to real-time, mass surveillance like that of Big Brother. Police have an incentive to collect as many photos as possible because the larger the database the more likely they are to get a match and solve a crime or identify a suspect or person of interest.

- Real-time, mass surveillance could also chill First Amendment speech unpopular with the government. Advocates point to the FBI's disgraced COINTELPRO program of surveillance against civil rights activists and Vietnam War protesters during the '60s and '70s.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available.

LEGAL QUESTIONS

While the courts have not yet addressed the following, they will. Law enforcement would serve itself well not to go into those cases with a record of overreaching, else the courts restrain us more than we might have effectively restrained ourselves.

1. Does a face recognition constitute a "search" that triggers Fourth Amendment protection?

2. What is the legal standard police must meet before using FRT?

3. Does your state have a law regulating the collection of biometric data?

4. Do your state courts offer more protection against government intrusion under your state constitution than the Supreme Court does under the U.S. Constitution? See, for example, an analysis of FRT under Utah case law as distinguished from the same analysis under federal case law.

PLAN AND CONSIDER

1. Consulting with your prosecutor about federal and state laws and court cases that might be relevant to police use of FRT.

2. Adopting FRT use policies and making them public. Here is a sample policy.

3. Training officers to ensure the most effective use of the scanners. The Institute of Electrical and Electronics Engineers (IEEE) Certified Biometrics Professional (CBP) program offers courses which set a baseline of biometric knowledge for those who plan to use FRT. These course standards aren't yet national but some agencies have adopted them as certification standards.

Law-abiding citizens are not against police use of FRT. Georgetown Law's Center on Privacy & Technology noted:

> *The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of*

> *good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.*

But the public has real concerns about FRT and privacy. Concerns we'd do well to consider in advance of court rulings.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags › Investigations • Legal • Warrants

Images not showing up? Click here

NCJTC National Criminal Justice Training Center of Fox Valley Technical College

Registration Open for 2017 Conference!

11th Annual National Conference on Responding to Missing and Unidentified Persons Conference

Multiple Victim Events: Implications for Investigation, Search, Rescue, and Recovery
September 19 - 21, 2017 | Atlanta, GA

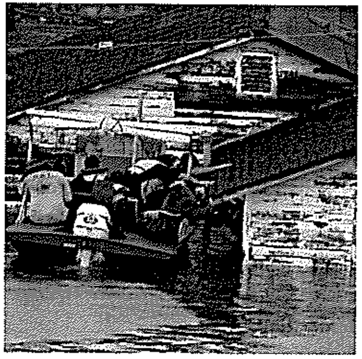
Individual Registration $400

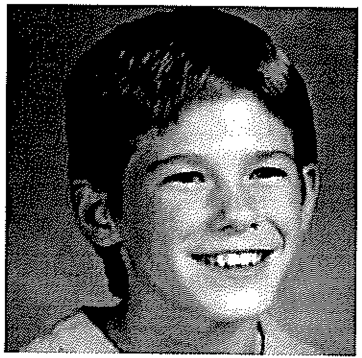
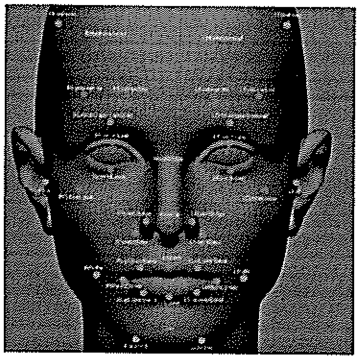
REGISTER

Groups of 3+ $350 per registrant

REGISTER

2017 Conference Highlights

Emergency Preparedness	FEMA Certification
	

Lessons Learned from Katrina	Emergency Ops Planning for Rural Jurisdictions
Panel Discussion	**Investigation Case Study**
 The Jacob Wetterling Story	 Barway Collins
Public Information	**High Tech**
 Managing the Media at Sandy Hook	 Using Facial Recognition Software

See our agenda for full details about the conference!

AGENDA

MORE INFO

Venue and Lodging

Sheraton Atlanta Hotel | 165 Courtland Street NE | Atlanta, GA
(404) 659-6500

MORE INFO

Questions? Please contact us at (888) 347- 5610 or email dcoffice@fvtc.edu

NCJTC
National Criminal Justice Training Center
Fox Valley Technical College

NATIONAL ASSOCIATION FOR SEARCH AND RESCUE
NASAR

National Criminal Justice Training Center
(855) 866-2582 | info@ncjtc.org | ncjtc.org | facebook.com/ncjtc

Fox Valley
TECHNICAL COLLEGE
Knowledge That Works

NCJTC, 1825 N. Bluemound Drive, Appleton, WI 54914

SafeUnsubscribe™ jlavalle@northamptonma.gov

Forward this email | Update Profile | About our service provider

Sent by info@ncjtc.org

POLICEONE.COM

Topics > 2017 Guide to Emerging Technologies > Articles

Cop Gumbo

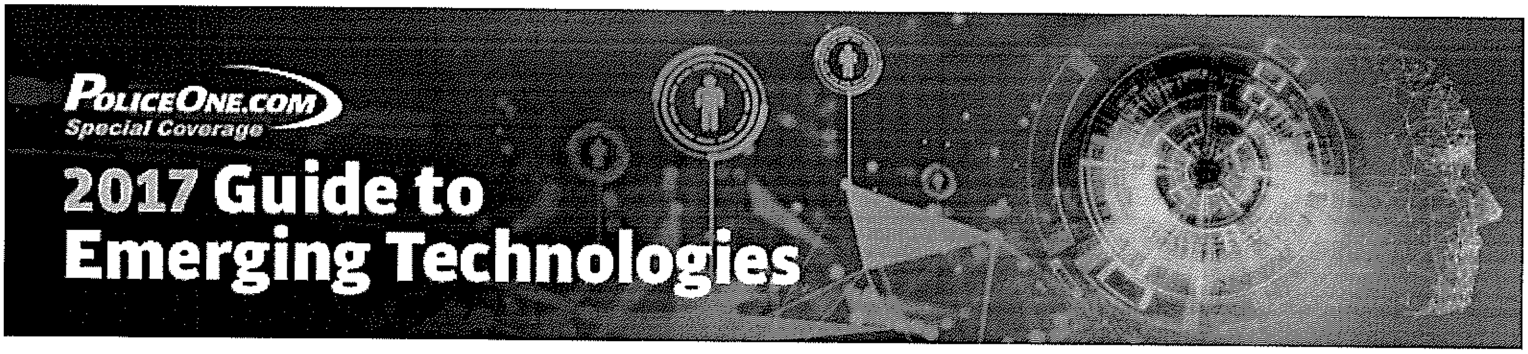
with Val Van Brocklin

Facial recognition technology and a 'reasonable expectation of privacy'

Law enforcement might consider using discretion before a court decides whether police need a warrant to scan someone's face

Editor's Note:

From crafting policy to tactical considerations, PoliceOne's **2017 Guide to Emerging Technologies** features expert analysis on soundwave technology, facial recognition software, handheld narcotics analyzers, the future of traffic stops, how constitutional law impacts the collection of data for investigations, and how advancements in biometric technologies will help improve correctional facilities.



Sept. 11 demonstrated that the greatest military might in the world couldn't protect us against the "asymmetric threats" of a few "unidentifiable enemies." The idea that FRT could identify terrorist suspects in public locations before they committed their crimes seemed to offer some protection.

Last May, the Government Accountability Office (GAO) issued a report about the FBI's amassing of 411.9 million facial images as part of its Next Generation Identification (NGI) program. It criticized the

programs secrecy and intrusion on privacy. Eighty percent of the photos were of people who had committed no crime. That's a significant police-created biometric database of primarily law-abiding Americans.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available. (Photo/Pixabay)

"If you're reading this in the United States, there's a 50 percent chance that a photo of your face is in at least one database used in police facial-recognition systems," reported the Atlantic Monthly last October.

Georgetown Law's Center for Privacy and Technology published a report the same month addressing the scale of local and state police involvement in facial recognition. The year-long investigation was based on more than 15,000 pages of records obtained through more than 100 FOIA requests. It found that police departments in nearly half the states can use facial-recognition software to compare surveillance images with databases of ID photos or mugshots. Some departments only use the technology to confirm the identity of a suspect who's been detained; others continuously analyze footage from surveillance cameras.

The GAO and Georgetown Law's reports are fueling public debate, which often lags behind evolving technology – as do court decisions. To date, I could find no court ruling on police use of FRT and the Fourth Amendment's reasonable expectation of privacy against government intrusion absent probable cause and a warrant.

PUBLIC DEBATE

Proponents of police use of FRT argue:

• There is no expectation of privacy to your face once you take it out in public.

• Any privacy intrusion is a small price to pay for increased public safety.

• What difference does it make if the government has a digital algorithm of your face they can use to ID you if you haven't done – or aren't doing – anything wrong?

Privacy advocates' concerns include:

• A reasonable expectation of privacy includes a reasonable expectation of anonymity from government use of computer algorithms and databases to capture law abiding citizens' faces and identify them without their knowledge or consent.

• FRT allows for a different kind of tracking that can occur from far away, in secret, and on large numbers of people. Fingerprints are only left on things you touch and you know when police are taking them. You can't leave your face at home and, with limited exceptions, it isn't acceptable to cover it. Depending how it's used, FRT could rob citizens of a reasonable expectation of anonymity.

Giving police the rights to do this without judicial oversight creates a slippery slope that could lead to real-time, mass surveillance like that of Big Brother. Police have an incentive to collect as many photos as possible because the larger the database the more likely they are to get a match and solve a crime or identify a suspect or person of interest.

- Real-time, mass surveillance could also chill First Amendment speech unpopular with the government. Advocates point to the FBI's disgraced COINTELPRO program of surveillance against civil rights activists and Vietnam War protesters during the '60s and '70s.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available.

LEGAL QUESTIONS

While the courts have not yet addressed the following, they will. Law enforcement would serve itself well not to go into those cases with a record of overreaching, else the courts restrain us more than we might have effectively restrained ourselves.

1. Does a face recognition constitute a "search" that triggers Fourth Amendment protection?

2. What is the legal standard police must meet before using FRT?

3. Does your state have a law regulating the collection of biometric data?

4. Do your state courts offer more protection against government intrusion under your state constitution than the Supreme Court does under the U.S. Constitution? See, for example, an analysis of FRT under Utah case law as distinguished from the same analysis under federal case law.

PLAN AND CONSIDER

1. Consulting with your prosecutor about federal and state laws and court cases that might be relevant to police use of FRT.

2. Adopting FRT use policies and making them public. Here is a sample policy.

3. Training officers to ensure the most effective use of the scanners. The Institute of Electrical and Electronics Engineers (IEEE) Certified Biometrics Professional (CBP) program offers courses which set a baseline of biometric knowledge for those who plan to use FRT. These course standards aren't yet national but some agencies have adopted them as certification standards.

Law-abiding citizens are not against police use of FRT. Georgetown Law's Center on Privacy & Technology noted:

> “ *The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of*

> *good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.*

But the public has real concerns about FRT and privacy. Concerns we'd do well to consider in advance of court rulings.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags › Investigations • Legal • Warrants

POLICEONE.COM

Police Products > Police Facial Recognition

Vigilant Solutions Facial Recognition Technology Overview

Vigilant Solutions' facial recognition technology suite includes FaceSearch and Lineup - two revolutionary products that are designed to be easy to use and affordable for agencies of all sizes.

Tags > Tech

DAY 1: APRIL 24, 2017

Session 1 (10:00am - 11:15am)	Session 2 (11:30am - 12:45pm)	Session 3 (2:30pm - 3:40pm)	Session 4 (3:50 - 5:00)
Tips & Tricks in High Tech Crimes (M. Menz, HPE & K. Loving, MSAB)		Successful Case Studies of Applying Big Data to Dark Web Investigation, Data Breaches, and Payment Card Breaches (D. Rogers - Terbium Labs)	Swatting, Doxing, & Cyber Investigations (D. Costantino, NJSP)
Video Examination for the Police Investigator (G. Fredericks, Forensic Video Solutions)	Surveillance/Wire Tapping (P. Hanley, MA AGO & M. King, FBI)	Microsoft Online Safety and LENS: Cybertips and Overviews (T. Ingle & S. Sulivan, Microsoft)	Intelligence Collections for Law Enforcement (K. Branzetti, DANY)
Live RAM Analysis: from Acquisition to Reporting (Y. Gubanov, Belkasoft)	Advances in Forensic Hardware (M. Kressel, Sumuri)	Windows 10 Privacy Tweaks (Herb Pittman, FLETC)	Social Apps in Smartphone Investigations (J. McQuaid, Magnet)
Accelerate Your Digital Investigations (R. Frawley, ADF Solutions)	Deep Diving for Forensic Gold – Applications, and Deleted Data (L. Reiber - Oxygen Forensics)	DVR Triage: Best Practices for Recovering Digital Video Evidence (P. Melaragni, MA AGO)	Case Studies: Discovering and Analyzing Digital Data Acquired from Motor Vehicle Systems and Connected Mobile Devices (D. Brister, Berla)
osTriage Update/Refresh (Part 1 of 2) (J. Rich, Plano Police Deprtment (TX))		Going Incognito: Simple Steps to Become Anonymous Online (T. Doyle, FBI)	
Investigating in the Cloud (J. Sedoski, NW3C)	The Dark Web: Tor-chlights Needed Past This Point (K. Petro, NW3C)	Open Source Intelligence Gathering (J. Sedoski, NW3C)	Virtual Currency: Dollar Dollar Bits Y'all (K. Petro, NW3C)
Blazing through Massive Amounts of Pictures and Videos (R. Navarro, Griffeye)	RAM: A "Real-World" Approach to Memory Acquisition & Analysis (J. Shackelford, PassMark)	OS X Native Analysis in a Virtual Environment (Limit 24) (J. Leech, FLETC)	
Twitter Investigations (J. Fitzsimmons & L. Wagner, SEARCH)		Autopsy Lab (B. Carrier, Basis Technology)	
SEARCH Investigative Resources (T. Lott & D. Chatfield, SEARCH)	Introduction to the Darknet (T. Lott & D. Chatfield, SEARCH)	Mac Forensic Imaging for Core Storage, Fusion Drives and FileVault (S. Whalen, Sumuri)	Advanced digital forensic training: from smartphone to cloud acquisition, from carving to SQLite forensics, and more (Y. Gubanov, Belkasoft)
Enabling Team Collaboration: Unifying Investigative Teams with the Right Information in the Right Format at the Right Time (J. Cole & A. Buxton, Cellebrite)	UFED Technology / UFED Reader (J. Cole & A. Buxton, Cellebrite)	Extracting from the Impossible: Working with Damaged Mobile Devices (A. Buxton & B. Morgan, Cellebrite)	Forensic Mobile Device Repair (A. Buxton & B. Morgan, Cellebrite)
Recovery of Video Evidence Using DVR Examiner (Hands-on) (Limited to 16) (B. Rolland-Keith, DME Forensics)		Forensic Audio Clarification Basics (B. Rolland-Keith, DME Forensics)	The Future of DVR Examiner – DVR Examiner 2.0 Preview (J. Schroering, DME Forensics)
Introduction to Forensics & Cyber (D. McSweeney, MSP & J. Fitzsimmons, SEARCH)	Authentication & Admissibility (H. Wise, Ventura County DAO)	Mobile Evidence Sources (L. Wagner, SEARCH)	Social Media Investigations (L. Wagner, SEARCH)
Tracing IP Addresses (G. Kessler, Embry-Riddle Aeronautical University)	IPv6 (G. Kessler, Embry-Riddle Aeronautical University)	ECPA & SCA (A. Abraham)	Legal Issues in the Cloud (A. Abraham)
Cyber Incident Triage (B. Carrier, Basis Technology)	The Consumer Sentinel Network: A Free Cybertool for Law Enforcement (N. Mastrocinque - FTC)	Cyber Security Panel (J. Emerson, IACP, M. Meglino, ODNI)	ATT NELOS Reports (S. Ray, Zetx)

▨ Lab	Lecture		

Day 2: APRIL 25, 2017

Session 5 (8:30am - 9:40am)	Session 6 (9:50am - 11:00am)	Session 7 (11:10am - 12:20pm)	Session 8 (2:15pm - 3:30pm)	Session 9 (3:45pm - 5:00pm)
HUMAN TRAFFICKING Spotlight (Kristin Boorse, Thorn)	HUMAN TRAFFICKING Illicit Massage Businesses (MA AGO - Human Trafficking Division)	HUMAN TRAFFICKING Traffic Jam (Cara Jones, Marinus Analytics)	HUMAN TRAFFICKING Demand Reduction (Angie Bayliss, CEASE Phoenix)	HUMAN TRAFFICKING Sex Buyer Stings (MA AGO - Human Trafficking Division)
CHILD EXPLOITATION Trends in Child Exploitation Investigations (J. Rich, Plano TX PD)	CHILD EXPLOITATION Proactive and P2P Investigations (J. Rich, Plano TX PD)	CHILD EXPLOITATION Interviewing in Child Exploitation Cases (J. Rich, Plano TX PD)	CHILD EXPLOITATION Diving Deeper: Big Data Analytics to Interpret EXIF in NCMEC's Child Victim Identification Program (S. Allwang, NCMEC)	CHILD EXPLOITATION Once the Shutter Snaps: From Victimization to Restitution (S. Allwang, NCMEC)
TERRORISM ISIS Tactics; Kids, drones, vehicles, and bombs; Are you ready? (K. Branzetti, DANY)	TERRORISM Being a Source in a Terrorism Investigation and How to Recruit Future Sources (Former Source)	TERRORISM Continued Rise of the Cyber-Jihadist (L. Alkouri, Flashpoint)	TERRORISM Starting your Intel Unit; Advanced Intel Collection Techniques (K. Branzetti, DANY)	TERRORISM Operational Cyber-Security Procedures and Techniques in Undercover Investigations (NYPD)
Microsoft Online Safety and LENS: Cybertips and Overviews (T. Ingle & S. Sulivan, Microsoft)	Facebook (J. Barry, Facebook)	Google (C. McGoff & A. Senese, Google)	Apple (K. O'Shea, S. Cazador & L. Olle, Apple)	Reaching Out, an Overview of Working with Industry and Building Relationships (S. Hyde, HTCC)
Introduction to Open Source Intelligence (OSINT) & Social Media (Limit 30) (B. Gavioli, MSP & E. Bradstreet, DHS)				
Open Source Intelligence Gathering (J. Sedoski, NW3C)	The Dark Web: Tor-chlights Needed Past This Point (K. Petro, NW3C)	Investigating in the Cloud (J. Sedoski, NW3C)	Virtual Currency: Dollar Dollar Bits Y'all (K. Petro, NW3C)	Open Source Intelligence Gathering (J. Sedoski, NW3C)
Determining Sources of Information for a Case (M. Menz, HPE)	Blazing through Massive Amounts of Pictures and Videos (R. Navarro, Griffeye)	Developing an IR Response Script for Log Collection and Memory Collection (M. Menz, HPE)	Driving your Investigation with Vehicle and Cell Phone Forensics (K. Loving, MSAB)	
Facebook Searching and Saving (J. Fitzsimmons & L. Wagner, SEARCH)			Wi-Fi Tools for Analysis and Geo-Location (WTAG) (R. Dauzat, FLETC)	
Introduction to WinFE (T. Lott & D. Chatfield, SEARCH)			Introduction to the Darknet (T. Lott & D. Chatfield, SEARCH)	Live Analysis: '5-Minute Forensics' in P2P Cases (J. Shackelford - Passmark)
Take the Driver's Seat with Advanced Cell Phone Analysis (A. Buxton & J. Cole, Cellebrite)	Advanced Smart Phone (A. Buxton & J. Cole, Cellebrite)	Trends in Digital Investigations - Optimizing the Investigative Workflow (R. Engler, Cellebrite)	Maximizing Digital Evidence and Overcoming Challenges (R. Colangelo, NCFI)	PC and Mobile Forensics Current Capabilities and Training Review (A. Buxton, B. Page, B. Morgan, NCFI)
Advanced DVR Analysis Case Studies (J. Schroering, DME Forensics)	Acquisition & Processing of Video Evidence with DVR Examiner & - INPUT-ACE (J. Schroering & G. Fredericks, DME Forensics)	DME Forensics	Recovery of Video Evidence Using DVR Examiner (Hands-on) (Limited to 16) (J. Schroering, DME Forensics)	
ECPA (A. Abraham)	Search Warrants & Non-Warranted Seizure (C. Diaz, Cumberland County DAO)		Forensic Hands-On for Prosecutors (C. Kelly, MA AGO)	
Report Writing (G. Kessler, Embry-Riddle Aeronautical University)	Search & Seizure of Digital Evidence (K. Connolly, Barnstable PD)		Search Warrants 101 (A. Portney, MA AGO)	Search Warrants 102 (A. Portney, MA AGO)
Human Hacking: The Art of Social Engineering (R. Harnish, GreyCastle Security	You've Been Hacked, Now What? (R. Harnish, GreyCastle Security)	Router Forensics (G. Kessler, Embry-Riddle Aeronautical University)	The Internet of Things: Understanding and Using IoT to Prove Your Case (J. Fitzsimmon & L. Wagner, SEARCH)	Deep and Dark on the Web (R. Comella, AccessData)
Introduction to i2 Enterprise Insight Analysis (EIA) (IBM)	Tips and Tricks for Analysts using i2 Analyst's Notebook (IBM)	Introduction to Intelligence Analysis using i2 Analyst's Notebook (IBM)	Cyber Crime - How To Stop Criminals From Getting Rich Without Getting Caught. (IBM)	Cloud Storage for Investigations/Law Enforcement (IBM)

Lab	Lecture			

DAY 3: APRIL 26, 2017

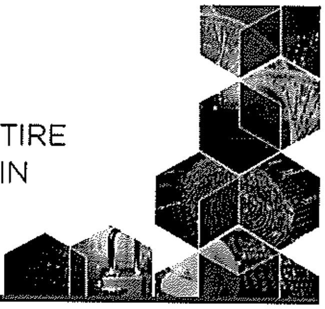
Session 10 (8:30am - 9:40am)	Session 11 (9:50am - 11:00am)	Session 12 (11:10am - 12:20pm)	Session 13 (2:15pm - 3:30pm)	Session 14 (3:45pm - 5:00pm)
Forensics on a Budget (M. Menz, HPE)	Memory Analysis with Magnet RAM Capture and Magnet AXIOM (J. McQuaid, Magnet)	Technical Aspects of Aaron Hernandez Investigation/Trial (J. Donovan, MSP)	Boston Marathon Bombing (K. Swindon & J. Petrozzeli, FBI)	How to Automate your Workflow and Data Analytics (B. Chou, Personable)
Ghost in Shell Items (D.Cowen, SANS)		Treasure Hunting for USB Gold (E. Dygert, SANS)	Meet SRUM (E. Dygert, SANS)	Artifacts of Online Information Exposure and Methods for More Effective Online Investigations (A. Barr, Digital Outcomes)
Basic Video Forensics for Investigators (G. Fredericks, Forensic Video Solutions)			Verizon PCMD-RTT Data (S. Ray, Zetx)	
Wi-Fi Tools for Analysis and Geo-Location (WTAG) (R. Dauzat,FLETC)		Windows 10 Privacy Tweaks (Herb Pittman,FLETC)	OS X Native Analysis in a Virtual Environment (Limit 24) (John Leech, FLETC)	
Investigating in the Cloud (J. Sedoski, NW3C)	Virtual Currency: Dollar Dollar Bits Y'all (K. Petro, NW3C)	Open Source Intelligence Gathering (J. Sedoski, NW3C)	The Dark Web: Tor-chlights Needed Past This Point (K. Petro, NW3C)	Investigating in the Cloud (J. Sedoski, NW3C)
OSForensics Triage Certificate Course (J. Shackelford, PassMark)			Hot Tub Forensic Time Machine (D.Cowen)	Released for Judicial Panel (Tiffany Ballroom)
BlueStacks for App Investigations (J. Fitzsimmons & L. Wagner, SEARCH)	Firefox Addons: Free Resources to Enhance your Investigations (J. Fitzsimmons & L. Wagner, SEARCH)	Become A Google Jedi: Save Yourself From Information Overload (J. Fitzsimmons & L. Wagner, SEARCH)	Emerging Technologies (J. Fitzsimmons & L. Wagner, SEARCH)	
Introduction to WinFE (T. Lott & D. Chatfield, SEARCH)			Digital Evidence Investigator (R. Frawley, ADF Solutions)	
CCME Prep Session (A. Buxton, B. Morgan, J. Cole Cellebrite)	Preparing to Testify Digital Evidence in Court (R. Engler, Cellebrite)	Technology in Terrorism and Counterterrorism (M. Hassan, Cellebrite)	Undercover Device Evidence: Accelerating Social Network Investigations (R. Engler, Cellebrite)	Social Network Investigations (A. Buxton & J. Cole, Cellebrite)
The Future of DVR Examiner – DVR Examiner 2.0 Preview (J. Schroering, DME Forensics)	Vehicle Make/Model Determination (B. Rolland-Keith, DME Forensics)	Cell Towers, Cell Phones, and Video Surveillance: Bringing Evidence Together for the Courtroom (K. Connolly, Barnstable PD)	Uber for Law Enforcement (W. Stormer & M. Sullivan, Uber)	Released for Judicial Panel (Tiffany Ballroom)
Trial Prep | Experts, Evidence & Multimedia Exhibits (Part 1) (A. Yas & C. Crawford, Norfolk DAO)	Trial Prep | Experts, Evidence & Multimedia Exhibits (Part 2) (A. Yas & C. Crawford, Norfolk DAO)	Hot Topics in Cyber & Digital Evidence (C. Diaz, H. Wise, D. McSweeney, C. Kelly)	Mock Trial: Direct & Cross (C. Diaz & H. Wise)	
4th Amendment/Particularity (C. Campbell, Suffolk DAO & J. Charles, Middlesex DAO)	Cyber Oral Argument (C. Campbell, Suffolk DAO & J. Charles, Middlesex DAO)	Interview & Interrogation (P. Curran, Norwood PD)	Expert Witness (J. Verner, Suffolk DAO)	
Understanding Google Location Information (S. Ray, ZetX)		Techniques and Strategies for Using Facial Recognition in Cyber Crime Investigations (R. Rodriguez - Vigilant Solutions)	Intelligence Collections for Law Enforcement (K. Branzetti, DANY)	

Lab	Lecture			

Email not displaying correctly? View it in your browser.

GCC FORENSICS
CONFERENCE & EXHIBITION
13- 14 NOV 2019 I THE GULF HOTEL BAHRAIN
مؤتمر ومعرض الخليج العربي للأدلة الجنائية

THE MUST ATTEND
EVENT FOR THE ENTIRE
FORENSIC SECTOR IN
THE MIDDLE EAST



CALL FOR PAPERS VISITING EXHIBITING CONTACT US

Join us in Bahrain for the third edition of GCC Forensics Conference & Exhibition

Dear Michael,

Find out more and submit a paper

On behalf of the **GCC Forensics scientific and organising committee**, we are delighted to invite you to submit a paper for the upcoming 3rd edition of GCC Forensics Conference due to take place this 13-14th November at the Gulf Hotel in Manama, Bahrain.

The event will be held for the first time in the Kingdom of Bahrain which promises to bring a range of new developments to our existing conference.

2019 Call for Papers

This event will bring together law enforcement, forensic scientists, experts, researchers and educators from around the world who are engaged in forensic science as well as related investigative and security fields. The purpose of the conference and co-located exhibition is to discuss the current state, and further developments of the sector through presentations, workshops, case study analysis, and panel discussions.

We are particularly interested in presentations covering the following topics:

- Terrorism-related crime handling from the crime scene to courtroom
- IED and CBNRe â€“ evidence handling, safety and identification
- Advancements in forensic DNA techniques and emerging technology
- Human identification, forensic medicine, and biological evidence preservation
- Forensic toxicology and drug control
- Digital forensics and cybersecurity in the Middle East
- Facial recognition, AI and other cutting-edge technology applied to criminal investigation
- Innovation in casework and high volume laboratory management
- Future of crime scene investigation
- Multidisciplinary and complex case studies from across the globe

Other studies that may be related to overall conference scope will also be considered for presentation as long as they meet the main submission criteria.

Important Deadlines:

1 July 2019	Abstract submission deadline
1 August 2019	Final notifications sent to speakers
1 September 2019	Full slides deadline

All submissions must be uploaded to EasyChair, it requires users to create a profile to submit: http://info.clarion-defence.com/e/339191/conferences--conf-gccfc2019/5dmnm/133781996?h=GDe5jnXMkBbXyU-8roh2sVOAKQYKVVkYLPS9LJVr3yo

For full details, visit the **GCC Forensics Website**.

We look forward to welcoming this November in Bahrain!

Kind regards,

Mariana Deâ€™ Carli
Content Manager, GCC Forensics Conference

Contact us

Conference

Sales & Sponsorship

Mariana De Carli
Content Manager
T: +971 (0) 4 4356101
M: +971 52 657 9856
E: mariana.decarli@clarionevents.com

Samar Yaafar
Senior Sales Executive
T: +971 (0) 4 4356101
M: +971 58 971 8800
E: samar.yaafar@clarionevents.com

Officially supported by
Bahrain Ministry of Interior

Media Partners

BIOMETRIC
UPDATE.COM

EVIDENCE
TECHNOLOGY MAGAZINE

FIU | FLORIDA
INTERNATIONAL
UNIVERSITY

LAB WORLD

Follow on Twitter Friend on Facebook Follow on Instagram

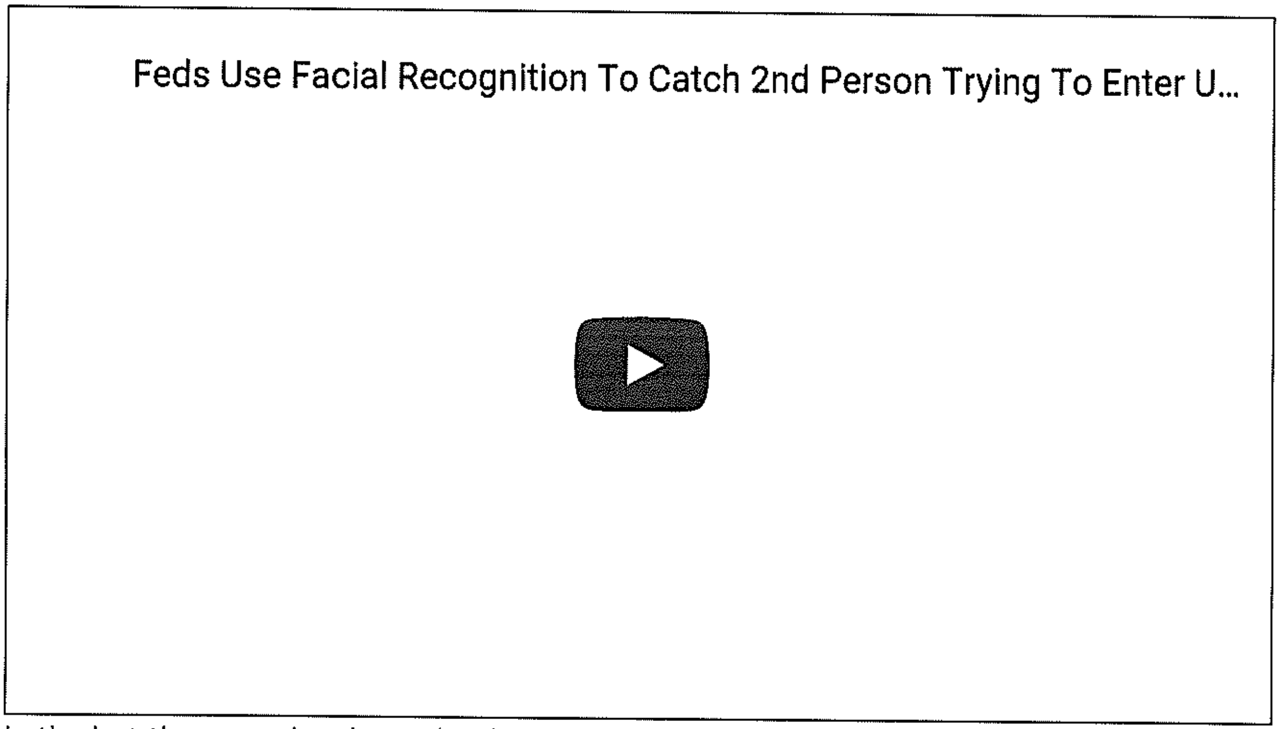
update subscription preferences or unsubscribe

Home // Investigations // Forensics // Facial Recognition // Feds Use Facial Recognition to Catch 2nd Person Trying to Enter U.S. Illegally

Feds Use Facial Recognition to Catch 2nd Person Trying to Enter U.S. Illegally

In the last three weeks, the technology at Washington's Dulles International Airport has been used to catch two imposters trying to illegally enter the U.S.

SEP. 12, 2018



Feds Use Facial Recognition To Catch 2nd Person Trying To Enter U...

In the last three weeks, the technology at Washington's Dulles International Airport has been used to catch two imposters trying to illegally enter the U.S.

Join the conversation!

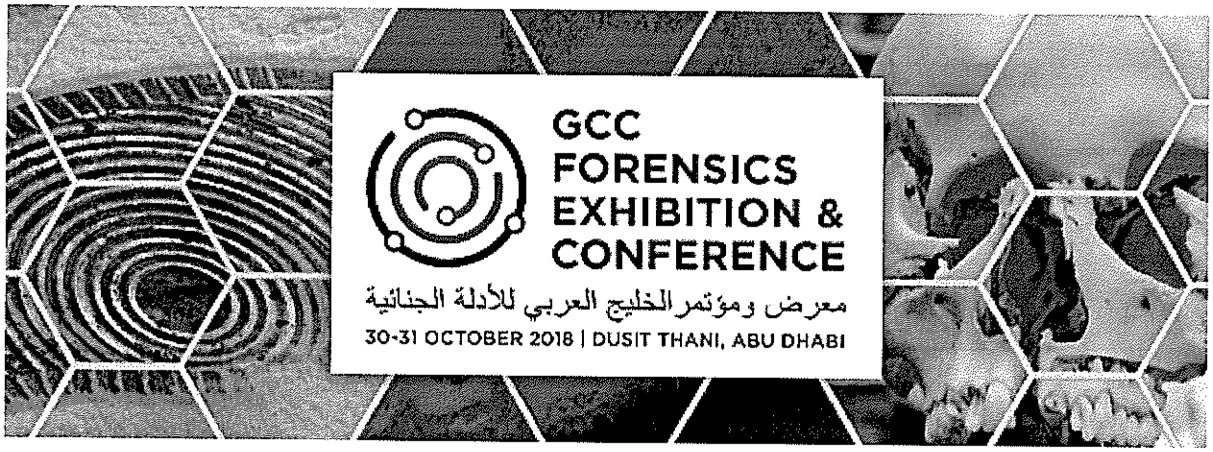
This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?

FACIAL RECOGNITION

Report: NYPD Using Celebrity Photos to Track Down Criminals

Email not displaying correctly? View it in your browser.


GCC
FORENSICS
EXHIBITION &
CONFERENCE
معرض ومؤتمر الخليج العربي للأدلة الجنائية
30-31 OCTOBER 2018 | DUSIT THANI, ABU DHABI

VISITING EXHIBITING CONTACT US REGISTER

Last chance to submit an abstract for the GCC Forensics Conference

The call for abstracts for the GCC Forensics Conference will close on **Monday 30th July**. Don't miss your chance to contribute to the must attend conference for the entire forensic sector in the middle east.

Find out more and submit a paper

GCC Forensics takes place 30-31 October 2018 at Dusit Thani Hotel Abu Dhabi, and features over 60 speakers across two conference streams. Over 50 suppliers to the forensic science community will also be located in the exhibition. **Register to attend today**.

REGISTER TO ATTEND

Conference Scope

The programme aims to discuss the most important and current topics in Forensic Science areas, with a particular focus on:

New technology & techniques for crime scene investigation	Complex & multidisciplinary crime solving

Workflow case management &forensic intelligence	Counterfeit currencies and documents
Criminal profile construction	Trends in forensic DNA & Next generation sequencing
Sex crimes & human trafficking investigations	Cold case solving
Investigation bias	Applied genomics in the context of forensics
Disaster victim identification	Facial recognition technology
Animal doping & exotic animal trafficking	CBRN-E and E-crime and cryptocurrencies
Evidence interpretation	Novel psychoactive substances
Cognitive forensic science	Environmental tools in time of death estimation
Bloodstain pattern analysis	Disaster victim identification
Forensic photography, audio and video examination	Fibres & trace evidence analysis
International forensic networks and information	Digital forensics applications for multidisciplinary investigations

Scope of the Conference

CSI, Forensic DNA analysis, Forensic Psychology, Trace Evidence, Future Forensic Technology, Criminalistics, Lab Management & Forensic Intelligence, DVI, Toxicology & Drug Control, Applied genomics, Forensic Pathology & Legal Medicine, Entomology, Forensic Anthropology , Forensic Archaeology, Wildlife Forensics & Animal Doping, Digital & cybercrime investigations, Questioned Documents & Counterfeit Currency, Forensic Odontology, Ethics & Bias, Ballistics, Forensic Engineering, Explosions and Fire investigations.

* We also welcome submissions from other areas of forensic science. Research may be rejected on the relevance criteria despite being of good academic quality, in order to maintain the consistency of the programme.

Find out more and submit a paper

Exhibiting at GCC Forensics Exhibition & Conference

The GCC Forensics Exhibition will provide you the opportunity to position your business in front of key decision makers and to an audience of senior forensic buyers and procurement professionals, all at one dedicated event.

There are a small number of stand spaces and sponsorship opportunities still available. **Get in touch** with the team today to request a floorplan or **download the event brochure**.

Contact us

Conference

Mariana De Carli
Content Manager
T: +971 (0) 4 4356101
M: +971 (0) 52 657 9856
E: mariana.decarli@clarionevents.com

Sales & Sponsorship

Maria Inez
Sales Manager
T: +971 (0) 4 4356101
M: +971 (0) 58 186 0617
E: maria.inez@clarionevents.com

Sponsors & Supporters

Gold Sponsor

LABWARE
Results Count

Gold Sponsor

integratedgulfbiosystems

Silver Sponsor

GE Healthcare
Life Sciences

Bronze Sponsor

Cellebrite

Bronze Sponsor

SAT
Scientific Analytical Tools

Lanyard Sponsor

MAGNET
FORENSICS

Supported by

شرطة أبوظبي
ABU DHABI POLICE

Supported by

INTERPOL

Knowledge Partner

جامعة خليفة
Khalifa University

Media Partners

OFFICIAL MEDIA PARTNER

999

Expert Witness™
Established 1996

DIGITAL
FORENSICS
/ MAGAZINE

myUAEguide

عين الرياض
Eye Of Riyadh

Worldwide Association of Women Forensic Experts
WAWFE

Counter-IED Report
www.counteriedreport.com

CRITICAL
INFRASTRUCTURE
PROTECTION
REVIEW

Cyber
Security
Review

LabBulletin

BIOMETRIC UPDATE.COM

EVIDENCE TECHNOLOGY MAGAZINE

Follow on Twitter Friend on Facebook Follow on Instagram

unsubscribe from all emails update subscription preferences

POLICEONE.COM

BRANDFOCUS

SPONSORED CONTENT FROM TOP POLICE BRANDS

Police Products > Investigation

How facial recognition solves cases in Indiana

The state fusion center helps local agencies develop leads and catch criminals using facial recognition from Vigilant Solutions

---

Sponsored by Vigilant Solutions

By Tim Dees for PoliceOne BrandFocus

What if you could identify a suspect from a powerful network of databases instead of just a single database? The Indiana Intelligence Fusion Center uses facial recognition technology from Vigilant Solutions to assist local, state and federal agencies in generating leads to identify persons of interest and solve crimes, large and small.

Facial recognition technology from Vigilant Solutions helps agencies identify persons of interest (photo/Vigilant)

Sgt. Jeff Carmin has spent most of his career in the more traditional roles of two city police departments and the Indiana State Police, performing traffic and criminal investigations throughout the state. He is now the director of operations at the Indiana Intelligence Fusion Center (IIFC) in Indianapolis.

WHAT IS A FUSION CENTER?

Fusion centers were established across the United States in the wake of 9/11 to create an information-sharing base among law enforcement agencies, whether federal, state, local or tribal. State and major urban area fusion centers provide information and intelligence to local agencies, working alongside federal agencies like the Department of Homeland Security and the Federal Bureau of Investigation to help local law enforcement.

The IIFC, operated by the Indiana State Police, leverages resources that would often be too costly for local agencies, said Carmin. It draws information from roughly 60 different databases and 72 other fusion centers around the United States.

The center also uses Vigilant Solutions for automated license plate and facial recognition technologies. Carmin said the center has used other facial recognition programs but none as successfully as FaceSearch from Vigilant Solutions.

"If you sent me a photo and the guy was looking to the side or down, or wasn't looking straight on like a driver's license photo, we weren't getting good results," he said. "What made us go with Vigilant, besides the cost, was the user-friendliness of it."

MATCHING MUG SHOTS IN THE DATABASE

The IIFC's experience with the Vigilant Solutions' facial recognition system improved significantly after they uploaded mug shot photos stored in Indiana's automated fingerprint recognition system into the comparison gallery maintained by Vigilant Solutions.

"Since then, we've had outstanding results when an investigator requests something via our facial recognition system," Carmin said. "There are just a little under a million booking records."

IIFC can also run comparisons against Vigilant Solutions' master gallery, which contains records from various Vigilant users around the country. Other image databases are available for comparison as well.

"The Department of Homeland Security has a site with multi-state facial recognition. We also utilize that for 30 different states that can run it against their different databases, whatever they may be," said Carmin.

HOW FACIAL RECOGNITION TECHNOLOGY WORKS

Whereas humans recognize faces by an analog method, computers do it by digital mapping. By measuring and comparing distances and angles between facial landmarks – like pupils, the corners of the mouth, the tip of the nose, the lowermost aspect of the chin, etc. – a face can be expressed as a digital pattern the computer can compare with other patterns.

When a sample photo is submitted for analysis in a facial recognition system, the system locates records with a similar pattern in the database and returns them to the user as possible matches.

Local investigators wanting to make use of the IIFC's facial recognition system upload photos or video still frames for comparison. An IIFC analyst enhances the photo, if necessary, using the Vigilant Solutions software, and the comparison results are sent back to the investigator, along with a log of enhancements made to the specimen image.

Vigilant Solutions' FaceSearch system can correct for various problems, such as an off-axis angle or poor image quality.

If the head is turned, you can actually get the head to turn to a more face front type of photo," Carmin said. "It will clear the photo up if it's a blurry photo, it will add eyes if the eyes need to be added and that type of thing."

SOLVING CASES BIG AND SMALL

Carmin recounts one success story where the IIFC assisted in a case where $7,000 in gift cards was stolen.

"The only photos available were two profile shots, both taken from video surveillance footage," he said. "Using the enhancement tools in the Vigilant software, an analyst was able to match the surveillance image to a booking photo of an inmate then housed in a county jail. The suspect was from Missouri and had no other ties to Indiana except that booking record. He also had outstanding arrest warrants."

Thanks to the image match from the Vigilant system, the suspect was identified at the county jail, served with the warrants and charged with the gift card theft.

"We've had a lot of success with this system," Carmin said. "It could be a homicide case, or it could range all the way down to a simple petty theft case."

Using a powerful technology to solve a shoplifting case might seem like overkill, but it illustrates how making a tool like facial recognition available to all law enforcement can improve satisfaction for all concerned (the gift card thief being a likely exception).

About the Author

Tim Dees is a retired police officer and the former editor of two major law enforcement websites who writes and consults on technology applications in criminal justice. He can be reached at tim@timdees.com.

POLICEONE.COM

Police Products > Police Facial Recognition

Policing Matters
with Policing Matters Podcast

The limitations and potential of facial recognition software

Police are using the software more and more to identify wanted criminals, missing people and suspected terrorists spotted on video

Download this week's episode on iTunes, SoundCloud or via RSS feed

Last year, rights groups and even Amazon employees and stockholders sought to stop that company from providing its Rekognition software to law enforcement agencies. By all accounts, that effort has failed, as police are using the software—as well as solutions from other vendors—more and more to identify wanted criminals, missing people and suspected terrorists spotted on video. In this podcast segment, Jim and Doug discuss the use of facial recognition technology, its limitations, and its potential for the future.

LEARN MORE

What police departments should consider before implementing facial recognition software

Facial recognition technology and a 'reasonable expectation of privacy'

Legal, privacy concerns to consider before implementing this scanning technology

How facial recognition solves cases in Indiana

Police Video Guide: The emerging tech, training and tactics shaping law enforcement

About the author

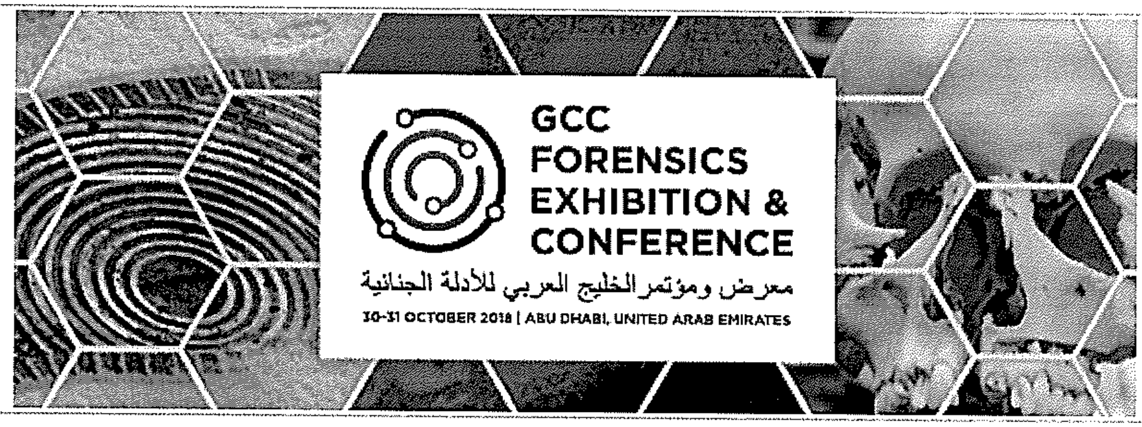
Talking the beat with leaders and experts on the PoliceOne police podcast.

In the Policing Matters Podcast, PoliceOne Senior Contributor **Doug Wyllie** and San Francisco Deputy Chief **Jim Dudley** (ret.) discuss current news, offer advice, thoughts, tips and laughs for officers. Have a topic you want discussed on the show? Send your comments and suggestions to policingmatters@policeone.com, and tune in every Friday for a new episode. Policing Matters is available for download on SoundCloud and via RSS feed.

Tags › Technology

The must attend event for the entire forensic sector in the Middle East

Email not displaying correctly?
View it in your browser.


GCC
FORENSICS
EXHIBITION &
CONFERENCE
معرض ومؤتمر الخليج العربي للأدلة الجنائية
30-31 OCTOBER 2018 | ABU DHABI, UNITED ARAB EMIRATES

Dear Michael

The GCC Forensics Exhibition and Conference organising and scientific committee has issued a call for speakers for 2018, the 2nd annual edition of the premiere forensics meeting in the region. The programme aims to discuss the most important and current topics in Forensic Science areas, with a particular focus on:

OFFICIALLY SUPPORTED BY

شـرطـة أبوظبـي
ABU DHABI POLICE

New technology & techniques for crime scene investigation	Complex & multidisciplinary crime solving
Workflow case management &forensic intelligence	Counterfeit currencies and documents
Criminal profile construction	Trends in forensic DNA & Next generation sequencing
Sex crimes & human trafficking investigations	Cold case solving
Investigation bias	Applied genomics in the context of forensics
Disaster victim identification	Facial recognition technology
Animal doping & exotic animal trafficking	CBRN-E and E-crime and cryptocurrencies
Evidence interpretation	Novel psychoactive substances
Cognitive forensic science	Environmental tools in time of

	death estimation
Bloodstain pattern analysis	Disaster victim identification
Forensic photography, audio and video examination	Fibres & trace evidence analysis
International forensic networks and information	Digital forensics applications for multidisciplinary investigations

Scope of the Conference

CSI, Forensic DNA analysis, Forensic Psychology, Trace Evidence, Future Forensic Technology, Criminalistics, Lab Management & Forensic Intelligence, DVI, Toxicology & Drug Control, Applied genomics, Forensic Pathology & Legal Medicine, Entomology, Forensic Anthropology , Forensic Archaeology, Wildlife Forensics & Animal Doping, Digital & cybercrime investigations, Questioned Documents & Counterfeit Currency, Forensic Odontology, Ethics & Bias, Ballistics, Forensic Engineering, Explosions and Fire investigations.

* We also welcome submissions from other areas of forensic science. Research may be rejected on the relevance criteria despite being of good academic quality, in order to maintain the consistency of the programme.

How to submit:

Click **HERE** for guidelines on how to prepare the abstract and paper ahead of the submission. Submit your abstract via:

http://info.clarion-defence.com/e/339191/conferences--conf-gccfec2018/y939/32188794 *No submissions will be accepted by email or other means for this year's Conference.

Important dates

- 12 July, 2018 - Speakers will be notified of acceptance
- 12 August, 2018 - Speakers must submit final **presentation slides**
- 30 August, 2018 - Deadline for submitting documents for speakers/substitute speakers

To register your interest in the event click **HERE**.

I will also be attending Forensics Europe Expo in London on 6-7 March – if you are attending and wish to discuss the conference at GCC Forensics Exhibition & Conference let me know.

On behalf of the scientific committee, we look forward to receiving your submission.

Kindest regards,

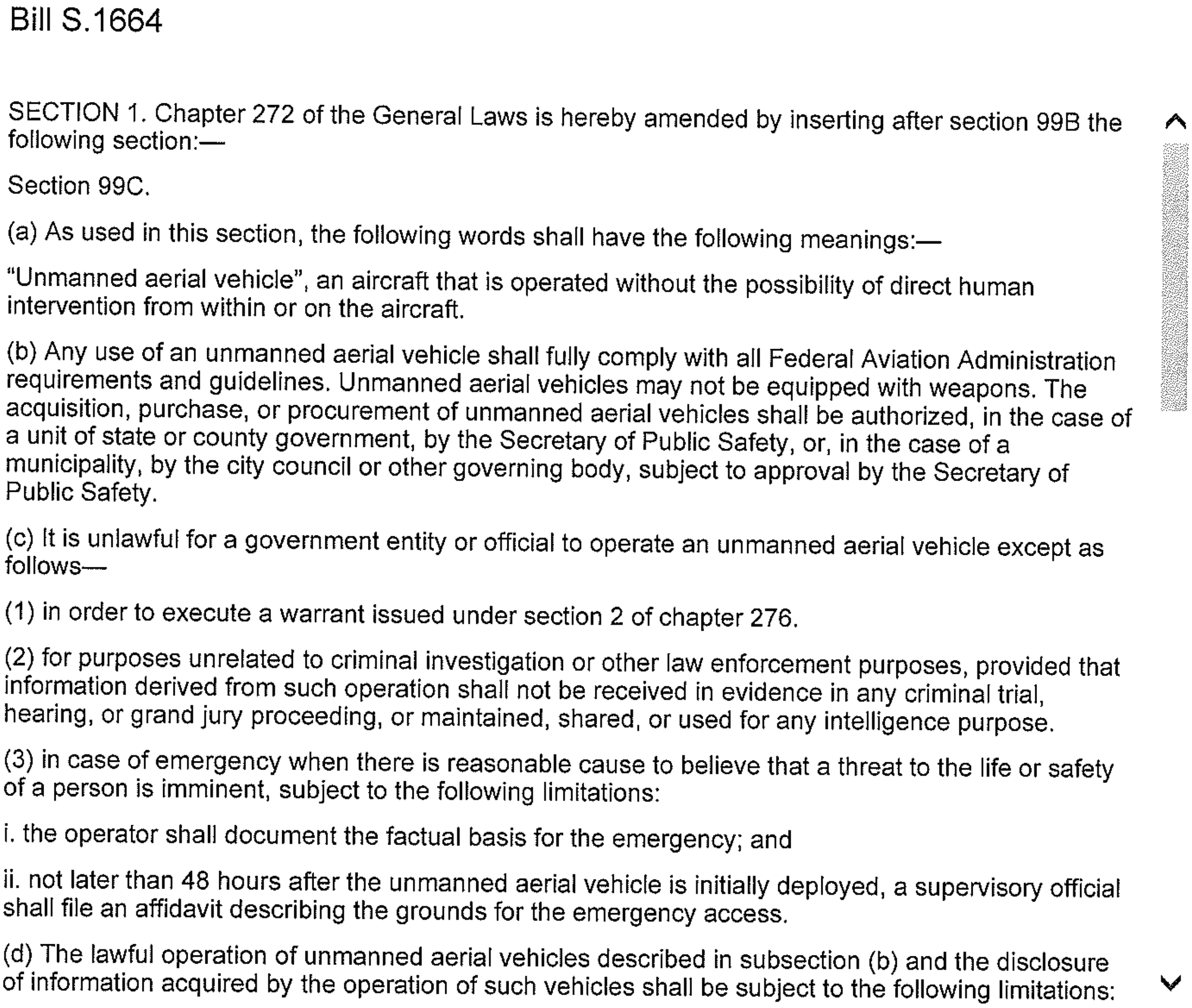
Mariana De Carli Al Ali
Content Manager
T: +971 (0) 4 4356101
E: mariana.decarli@clarionevents.com
W: www.gccforensics.com

GCC
FORENSICS
EXHIBITION &
CONFERENCE
معرض ومؤتمرالخليج العربي للأدلة الجنائية
30-31 OCTOBER 2018 | ABU DHABI, UNITED ARAB EMIRATES

Follow on Twitter Friend on Facebook Follow on Instagram

unsubscribe from all emails update subscription preferences

Please see the below bill in Massachusetts. The senate concurred and it is now in the Judiciary.



Bill S.1664

SECTION 1. Chapter 272 of the General Laws is hereby amended by inserting after section 99B the following section:—

Section 99C.

(a) As used in this section, the following words shall have the following meanings:—

"Unmanned aerial vehicle", an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

(b) Any use of an unmanned aerial vehicle shall fully comply with all Federal Aviation Administration requirements and guidelines. Unmanned aerial vehicles may not be equipped with weapons. The acquisition, purchase, or procurement of unmanned aerial vehicles shall be authorized, in the case of a unit of state or county government, by the Secretary of Public Safety, or, in the case of a municipality, by the city council or other governing body, subject to approval by the Secretary of Public Safety.

(c) It is unlawful for a government entity or official to operate an unmanned aerial vehicle except as follows—

(1) in order to execute a warrant issued under section 2 of chapter 276.

(2) for purposes unrelated to criminal investigation or other law enforcement purposes, provided that information derived from such operation shall not be received in evidence in any criminal trial, hearing, or grand jury proceeding, or maintained, shared, or used for any intelligence purpose.

(3) in case of emergency when there is reasonable cause to believe that a threat to the life or safety of a person is imminent, subject to the following limitations:

i. the operator shall document the factual basis for the emergency; and

ii. not later than 48 hours after the unmanned aerial vehicle is initially deployed, a supervisory official shall file an affidavit describing the grounds for the emergency access.

(d) The lawful operation of unmanned aerial vehicles described in subsection (b) and the disclosure of information acquired by the operation of such vehicles shall be subject to the following limitations:

On Tue, Jan 16, 2018 at 6:42 PM, Jonathan <jon@jrupprechtlaw.com> wrote:

> The FAA is getting sued...again. This time to the tune of $840 million. The case is Taylor v. FAA and Huerta. This is NOT John Taylor who was instrumental in having the drone registration regulations vacated in the Taylor v. Huerta case. Just to mention, I'm NOT involved in this case. This is a class action lawsuit (of at least 836,796 members who registered their drones) against the FAA. They are seeking $1,000 in statutory damages for **EACH** of the members of the class.
>
> Continue reading.......
>
> Unsubscribe | 2811 Grande Parkway, Suite 113, Palm Beach Gardens, FL 33410

--
Respectfully.

Michael J. Allard #106
Highway Safety Officer
Crime Scene Services
AFIS Administrator

POLICEONE.COM

Topics > Policing in the Video Age > Articles

Cop Gumbo

with Val Van Brocklin

As commercial use of facial recognition expands, what are the implications for police?

If citizens willingly permit widespread use of FRT outside of law enforcement, you could argue they no longer have any reasonable expectation of facial privacy

Editor's Note:

Few forces are impacting law enforcement like video. **Policing in the Video Age**, P1's yearlong special editorial focus on video in law enforcement, aims to address all facets of the topic with expanded analysis and reporting.

In the final installment of this four-part signature coverage effort, we take a look at the future of video in policing. Click here to learn more about the project.

Also be sure to check out our latest PoliceOne Digital Edition – **2018 Police Video Guide: The emerging tech, training and tactics shaping law enforcement** – in which we explore how departments can best utilize emerging video technologies to enhance police officer safety and improve operational efficiencies. Download the free guide here.

POLICING IN THE VIDEO AGE
What is the future of video in policing?
PoliceOne Signature

Facial recognition technology (FRT) is a software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours.

The Fourth Amendment protects people from warrantless government searches or seizures where they have a subjective expectation of privacy that is deemed reasonable by public norms. The reasonableness standard is decided on the totality of circumstances.

In this Friday, Nov. 3, 2017, file photo, an Apple employee demonstrates the facial recognition feature of the new iPhone X at the Apple Union Square store in San Francisco. (AP Photo/Eric Risberg, File)

This is why the expanding commercial use of FRT is interesting. If citizens willingly permit widespread use of FRT outside of law enforcement, an argument could be made that they no longer have any reasonable expectation of facial privacy.

EXPANDING COMMERCIAL USES OF FACIAL RECOGNITION SOFTWARE

In 2008, Lenovo released a line of laptops that allowed users to log on using their face instead of a password. Windows 10 does the same.

Facebook, Apple and Google use facial recognition to assist in "tagging" images – identifying someone in a photo by name.

Other online services that have used facial recognition include:

- Face recognition search engines;
- Stylecaster – a website that allows women to upload their image and try on different makeup, clothes, and hairstyles;
- Snapchat – An image messaging app that allows users to apply lenses to photos using FRT

In 2012, 20 percent of all smartphones shipped had facial recognition capability. It's estimated that by this year, 665 million smartphones and tablets will include facial recognition.

In 2015, China unveiled the first facial recognition ATM. Facial recognition has been incorporated into smart TVs by LG, Samsung and Panasonic. The TV set offers menus based on who's watching. The Nielsen company is exploring the use of smart TVs for measuring ratings and determining who's watching shows and ads.

into accounts. Similarly, Amazon filed a patent in March 2016 for a program that will allow users to authorize purchases by taking selfies.

Retailers are increasingly using the technology not just to prevent loss by identifying shoplifters but to improve sales by tracking legitimate shoppers. The Atlanta-based ad agency Redpepper is testing their project -- Facedeals. Users grant Facedeals access to their Facebook; Facedeals then learns the user's face. The idea is that stores, bars and restaurants rigged with Facedeals cameras will "recognize" users who have opted into the program – and will text a customized coupon to the user's phone based on their social media activity.

PUSHBACK AGAINST FACIAL RECOGNITION USE IN THE COMMERCIAL SECTOR

In Orwell's dystopian novel, "1984," everyone knew they were being watched and recorded by "The Party." The leader of The Party was called "Big Brother." From that came a pop culture phrase -- "Big Brother is watching you." It was my generation's metaphor for government intrusion.

But in 2013, one of the pioneers of FRT, Joseph Atick, told 60 Minutes, "Big Brother is no longer big government; Big Brother is big business."

More recently, the movie "The Circle" based on Dave Eggers' book imagines an alarming reality where everyone's personal information is readily shared and available on the internet. The Circle (a thinly-veiled, fictitious Facebook, Amazon and Google combined) would eliminate the need for search warrants.

The FBI's amassing of 411.9 million facial images for its Next Generation Identification (NGI) program has garnered plenty of media attention, but that lags well behind Facebook's 1.65 billion users. Facebook has the largest biometric database in the world – "and it's all been formed by people voluntarily submitting pictures to Facebook and identifying who they belong to," says Amie Stepanovich, director of the domestic surveillance project at the Electronic Privacy Information Center in Washington, D.C.

Facebook has refused to answer questions about what it does with its facial recognition information. Social media companies rarely talk about their internal systems. But in 2012, Facebook bought Face.com, whose company's founders had published a paper titled "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition."

Like the FBI's NGI program, the commercial sector's use of FRT is getting pushback. In 2014, the U.S. Department of Commerce held talks about whether and how commercial FRT should be regulated. The negotiations included representatives from consumer-advocacy groups and the tech industry. User privacy groups, including Electronic Frontier Foundation and the Consumer Federation of America, walked out. The industry and its lobbyists, they said, wouldn't even admit that users might want to consent to facial-recognition software so it was no use participating in the talks.

Recently, the Illinois Biometric Information Privacy Act has become the basis of a number of lawsuits against tech giants Facebook, Google, Shutterfly and Snapchat, with consumers claiming their biometric information was handled illegally.

One of the most-watched suits is that of three Illinois plaintiffs against Facebook, alleging the tech giant's collection, storage and subsequent use of biometric information without informed consent invaded their privacy. That case is making its way toward trial – or a settlement.

In Europe and Canada, privacy advocates won a victory last year when Facebook launched its photo app, Moments, without facial recognition scanning.

Plenty of Americans still feel they have some privacy rights to their faces – at least from being identified without their consent by businesses or the government. I wonder what they'll do if Facebook refuses to back down and tells them they can always opt out of Facebook. I wonder what they'll do when TSA offers a quick pass based on facial recognition to those who voluntarily participate, or retailers offer them discounts based on FRT.

If law enforcement waits awhile, the norm may well be that citizens have dealt away their facial privacy rights.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags › Legal

PoliceOne.com

Police Products > Police Facial Recognition

Cop Gumbo

with Val Van Brocklin

What police departments should consider before implementing facial recognition software

Police agencies need to know how to vet the technology and its vendors

In Orwell's dystopian novel, "1984," every citizen knows they're being watched. There are telescreens everywhere recording them. According to "the Party," this surveillance is for the betterment of the state as a whole, and citizens who resist or disobey are labeled traitors and disappear. The leader of the Party goes by "Big Brother."

The classic novel was assigned college reading for me. "Big Brother" was part of my pop culture lexicon – a synonym for government abuse of power as it related to civil liberties, often through mass surveillance. Today, watching, cataloging and identifying citizens aren't science fiction.

HOW FACIAL RECOGNITION SOFTWARE WORKS

NIST computer scientist Ross Micheals demonstrates a NIST-developed system for studying the performance of facial recognition software programs. (Photo/Robert Rathe)

Facial recognition software aims to identify or authenticate individuals by comparing their face against a database of known faces and looking for a match.

First, a computer must find the face in the image. Then it creates a numeric representation of the face based on the facial features. Finally, this numeric "map" of the face in the image is compared to database images of identified faces, for example, a driver's license database. There are almost as many computer algorithms for this process as there are companies.

Facial recognition has become more sophisticated in recent years.

Three-dimensional (3-D) facial recognition uses 3-D sensors to capture information about the shape of a face. Three-dimensional data points from a face vastly improve the precision of face recognition. One advantage of 3-D face recognition is that it's not affected by changes in lighting. It can also identify a face from a range of viewing angles, including a profile.

In 2015, Facebook announced its algorithm could identify people in unclear images or images in which people were not looking directly at the camera. Recently, according to Facebook's AI department, it doesn't even need a face but can identify people through hairdos, postures, gestures and body types.

Facial recognition accuracy depends on the algorithm used. In 2010, the U.S National Institute of Standards and Technology (NIST) tested various facial recognition systems and found that the best algorithm correctly recognized 92 percent of unknown individuals from a database of 1.6 million criminal records.

Currently, systems can reach reliability of up to 99 percent, depending on the image. It's more reliable than recognition by humans. In 2014, a study of border control officers with specific education and training in facial recognition found that fraudulent photographs were accepted in 14 percent of cases.

PUBLIC DEBATE OVER THE USE OF FACIAL RECOGNITION

Two recent reports have shined a spotlight on concerns about the accuracy and reliability of facial recognition. Both have received media attention.

In May 2016, the Government Accountability Office (GAO) issued a report on the FBI's Next Generation Identification (NGI) program which is amassing multimodal biometric identifiers such as face-recognition-ready photos, iris scans, palm prints and voice data, and making that data available to other agencies at the state and federal levels. The report criticized the NGI for its lack of transparency, absence of reliability testing and invasion of privacy.

In October 2016, Georgetown Law's Center for Privacy and Technology published findings from a year-long investigation based on over 15,000 pages of records obtained from over 100 FOIA requests. The report set out to inform the public about how facial recognition is used and the policies that govern how police can use it. Information about the FBI's use of facial recognition had been known. This report tried to tackle the scale of local and state law enforcement involvement.

Concerns about the reliability and accuracy of facial recognition include:

- While companies marketing the technology claim accuracy rates higher than 95 percent, the algorithms used by police are not required to undergo public or independent testing to determine accuracy or check for bias before being deployed on everyday citizens.

- Accuracy rates are not equal across algorithms. According to NIST, algorithms developed in China, Japan and South Korea recognized East Asian faces far more readily than Caucasians. The reverse was true for algorithms developed in France, Germany and the United States.

Facial recognition systems are more likely either to misidentify or fail to identify African Americans, errors that could result in innocent citizens being marked as suspects in crimes. Little is being done to correct for the bias. One study co-authored by a senior FBI technologist found that Cognitec, whose algorithms are used by police in California, Maryland and Pennsylvania, consistently performed 5-to-10 percent worse on African Americans than on Caucasians. One algorithm, which failed to identify the right person in 1 out of 10 encounters with Caucasian subjects, failed nearly twice as often with African Americans.

- This bias is compounded by the disproportionate number of African Americans who are surveilled, stopped, booked and have mug shots taken by police. (This isn't to say the algorithms are intentionally "racist." Rather, they are flawed on racial lines, probably unintentionally during the algorithms' development. An algorithm flaw in Google's facial recognition tagged two African Americans as "gorillas.")

- Facial recognition software often provides a list of possible matches. Police departments largely rely on officers to decide whether a candidate photo matches one in the list. A recent study showed that, without specialized training, humans make the wrong decision about such a match half the time.

- Face recognition systems aren't audited for misuse. Of the 52 police agencies queried in the Georgetown Law study, only nine (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, the Michigan State Police, provided documentation showing their audit regime was actually functional.

HOW POLICE DEPARTMENTS SHOULD PLAN FOR THE USE OF FACIAL RECOGNITION

There are several steps police departments should take when using facial recognition software:

- Police agencies are well-placed to require that facial recognition software vendors submit to NIST's existing accuracy tests and any new tests that it develops. Require vendors to address their algorithms' race, age and gender bias with accuracy tests and performance results.

- Provide training for officers who will be deciding whether there is a match amongst a list of possible candidates provided by facial recognition software.

- Log and audit the use of agency facial recognition software.

- Be transparent with your community about your facial recognition software, the vendor, accuracy testing, logging and auditing procedures.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags > Command Staff - Chiefs / Sheriffs • Legal

Mike... let me know what u think...

Captain John D. Cartledge
Operations Division Commander
Northampton Police Department
29 Center St
Northampton, MA 01060
413-587-1100(Dispatch)
413-587-1176(Office)
413-587-1137(Fax)
www.northamptonpd.com

Begin forwarded message:

> **From:** Jessica Berger <jsberger@outlook.com>
> **Date:** April 14, 2017 at 16:11:48 EDT
> **To:** "jcartledge@northamptonma.gov" <jcartledge@northamptonma.gov>
> **Subject: Transcript**
>
> Dear Captain Cartledge,
>
> Thank you and Officer Allard for so generously donating your time today. It will go a long way towards improving my research.
> Below is the rough transcript. Feel free to make edits anywhere you deem appropriate.
> The highlighted area in particular would benefit from attention.
> I will keep you updated about the final project and make sure to incorporate your changes.
>
> Thank you again. Have a good Easter.
>
> Respectfully,
> Jessica Berger
>
> This rough transcript is an interview conducted by Jessica Berger, MLIS candidate from SJSU with Northampton MA Police Captain Cartledge and Officer Allard, who generously donated their time to help with the foregoing research project about drones.
>
> Text in brackets ( ) indicate either added words to clarify - or to note where the audio was unclear and caused some confusion during the transcription process.
>
> *How did you get started working with drones?*
> Drones in our industry have become a little more popular as far as search and rescue tools and investigative tools. You think of deploying a helicopter from an hour and a half away at thousands and thousands of dollars and then the ability to get a more inexpensive way to actually look for people- we get a lot of missing people who are victims in the woods... (We try to look for) the best investigative (methods). (Using drones we can) find lost people, (take) aerial photos of accidents, find evidence you

can't find from the road. We assist the DPW with vegetation loss and help firefighters (by) giving them an aerial view.

(The drone program) started in January (of 2017?) we came up with a lot of research, policies, procedures and (obtained) approval from the government.

I'm an FAA licensed pilot and Seargeant Moody is licensed. This has been used throughout the (country). You get to see what an impressive tool this is.

(When using drones) we're coming from a 12 minute deployment - if we are on duty. So it's a quicker deployment than waiting for the State Police, which could take hours depending on the weather.

What about kidnapping?
It's hard to say with particular cases. We don't have FLIR, (which is) thermal imaging.

(With FLIR) You will see a body signature if you have someone in the woods (which otherwise) would be hard to see through the trees. But with thermal imaging you can see people lost in the woods

What are some of the drone initiatives right now?
We are currently working with the DPW (The Department of Public Works) doing aerial shots for them in areas they are concerned with and used (these aerial shots taken by drones) on crime scenes; a lot of training flights; one of them is marshland they have problems with beavers. You can't walk out there to get an aerial view of the beaver dam.

About obtaining drones:
(???Anyone well cit. can buy drones over age 13 register if the weight of the drone 5.5. or higher all have to be registered with FAA all regulations are posted there.
???FAA part 107 governs how drones are operated, which need registered???)

Can you explain the data collection policies?
All digital media evidence (DME) policy regulates that and audit procedures all strictly written digital media all video and images, we have policies that I may have a policy in A that derives for policy in B- they work together.

Do police use drones equipped with facial recognition apps?
A: No, these are not equipped (with facial recognition apps) in the police industry. You will not see that in law enforcement

J: I think for people with privacy concerns that is a big reassurance

Our drone doesn't have that (facial recognition) capability and under the guides of police association, that is clearly spelled out.

The records management (department provides) the policies I already talked to you about. All the policies are on the website and the new public records law changed recently and I'm not sure how that impacts the digital requests from the people

Someone sends or denies it.

Do you have an opinion about legislative changes that should be made regarding drones?
I would not personally say thoughts on rules but all pilots should abide by the FAA regulations. The FAA came up with (new) ones in Aug 2016 and March 2017 they are very informative and strict enough. There wouldn't be anything I would change; you will see them get stricter. The FAA has a piloting command that (the drone) has to be piloted for police or someone under direct control by the pilot.
(For hobbyists) all you have to do is register the drone you don't need a pilot liscense, you have to take a certification exam. You just have to register the drone but you have to abide by the regulations (about) air space, flying over people, everything that is in the regulations- or be fined.

What if people don't abide - will there be people not abiding by regulations, not police, but citizens, in the same way automobile drivers break rules?
You will always have that but in our agency we haven't run across anyone to report to the FAA. So if someone is flying over a crowd, we report them to the FAA and they get fined. That is not within (our) domain, we are agents of the federal government so we report to them.

How do you identify them?
You identify by asking, when you register a drone whether you have 1 or 10 you have a number put on a drone, the FAA looks at the number and then identifies it (correlates the number of the drone) to the person because it's a registered aircraft.

600,000 drones are predicted to be purchased this year, how might it affect your workload?
A: I don't think it will affect our workload, but it will (impact) the government's, and they will be restricting (drone policy more strictly). They are coming up with technology that aircraft can id drones - and something that will allow aircraft to id drones.

What is your opinion about criminals hacking Smartphones ?
A: The drones aren't Bluetooth enabled, I can't comment
(Our) drone doesn't have that capability. (Ours use) wifi from the remote to the drone and tablet they are using (on the ground). People are coming out with ways to hack drones and take over the phones. But we have the federal government and large corporations being hacked. What's the focus of your paper?

J: Drones as an information security tool because they are up and coming.

Are we the only police dept you are talking to?
As far as I know but wanted to talk to a programmer and the military.

Do you have an opinion about Sky grabber hacking the US military drones that could interfere with a mission. It is a 26 dollar software.
A: I have no idea. (Note- I will leave this out)

They show me the drone.

This is the phantom 4 DJI is the company this is the one we just got; there are different models and prices. This whole set up cost about 1200 dollars - not that expensive – operated gimble system as you fly you move the camera up and down it will do stills and video and it communicates to the remote to the tablet the video what's sent isn't always great. There's an sd card.

Q: To become airborne – how can it take off and stay aloft?
Captain Cartledge and Officer Allard show that the propellers are detached from the craft, which is why at first it looks impossible for it to take off...
A: The computer system is incredible, (there are) top and bottom sonars - it knows its latitude and longitude and where it is; if we lose a signal it will return to where it took off. It knows its GPS position - it wouldn't give us the victim's GPS but would allow us to id that person's place and its flow in direct eyesight. We always know where it is based on the line of site - we have to keep it in our line of sight at all times.

Some of the smaller ones called the Mavic pro foldable can go 3 miles but the FAA still says you need to maintain line of sight.

Every time we fly we have 2 people -we have a pilot in command and a visual observer relaying to the pilot if there are any hazards or harm. If (there is a traffic) accident (we) can stay away but just view (it) from the outskirts. From the tree line we don't have to be right on top -we are standing still from the line of sight. It is pretty strictly regulated.

Q: Are you experimenting with any other technology tools?
A: In general we are a pretty progressive department. We have a lot of other things other agencies have done. We have in-housie AFIS fingerprint systems; we have a ton of things -we have criminal investigation tools others don't have. Our website is informative, but we don't put out everything about our tools (such as the most up to date ones used at a crime scene. (We have) UTD LIDAR (light detection and ranging) – (it is) light detection (in lieu of radar?) We're always looking ahead at tech and it is expensive to (keep up).

Q: Exploring preparations for acquiring drones.
We did it the right way (the preparation for drones). We're an accredited agency - we have policies for everything -we crafted drone policy before we went forward and before we even bought the drone. We try to do things the right way.

J offers to give transcript and asks about the transcript being on the web
Obtains spelling: Allard.

What's the time frame on the paper- I'd like to read it just for my own, send it before you (submit it to your teacher).

Do you want to not have your names in there?
You are the pilot I don't care. When you write this make it clear that all we are doing are under the jurisdiction of the FAA, get it to us before deadline and we can change it I don't want to jeopardize license.

View Online

HEZBOLLAH, ISLAMIC STATE THREATEN HOMELAND SECURITY WITH PRESENCE IN LATIN AMERICA

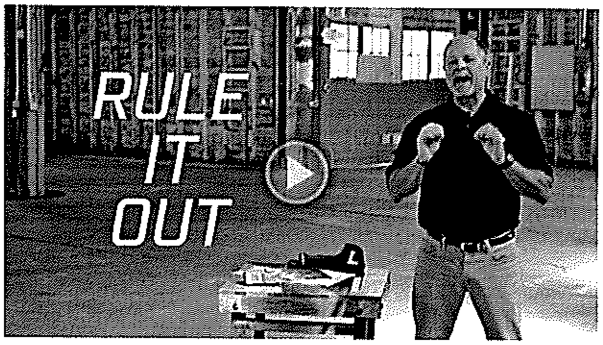
AUGUST 7TH, 2017

HOW TO KEEP YOUR ENTERTAINMENT VENUE SAFE FOLLOWING TERRORISM

[redacted]

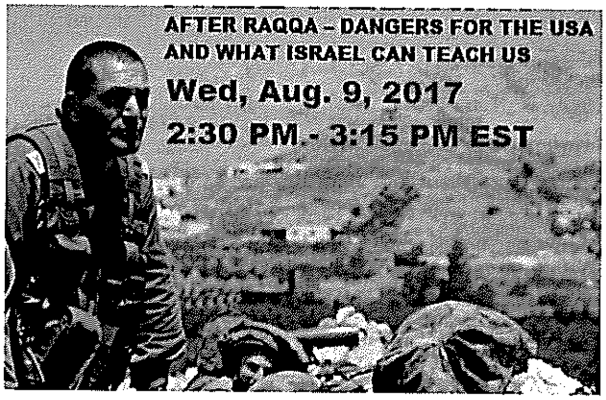
Customized Training

Sydney Terror: 'It Was As Close To A Major Attack As We've Ever Come'



AUGUST 9TH WEBINAR: AFTER RAQQA – DANGERS FOR THE USA AND WHAT ISRAEL CAN TEACH US

FREE WEBINAR



AFTER RAQQA – DANGERS FOR THE USA AND WHAT ISRAEL CAN TEACH US

Wed, Aug. 9, 2017

2:30 PM - 3:15 PM EST

Learning From Israel

Terrorists In Sinai Up Their Game

Join SSI's Israel Mission

Hezbollah, Islamic State Threaten Homeland Security With Presence in Latin America

The Counter Terrorist presents Homeland Security Professionals Conference and Exposition

Toronto Police Service Operations Centre (TPOC) Role In Fighting Terrrorism

The Terrorist Cop

Register Today And Save

GERMAN POLICE TEST FACIAL RECOGNITION CAMERAS AT BERLIN STATION AMID ATTACK FEARS

PVB

Portable Vehicle Barrier

PVB Objectives

Request More Information

Phone: (866) 573-3999 | Fax: (786) 573-2090
Address: 13155 SW 134th St., Suite #103, Miami, FL 33186
Email: Contact@homelandsecurityssi.com

Home // Investigations // Forensics // Facial Recognition // SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server uses deep neural network technology to provide facial recognition and tracking capabilities for surveillance video management systems.

NEUROTECHNOLOGY — JUNE 20, 2017

VIEW GALLERY

SentiVeillance Server is a ready-to-use solution that integrates with surveillance video management systems (VMS). Based on the company's deep neural network technology for facial recognition from surveillance camera video, SentiVeillance Server enhances VMS with advanced capabilities, such as the ability to quickly and accurately recognize faces in video streams and trigger analytical event notifications whenever an authorized, unauthorized or unknown person is detected. This greatly improves the workflow of VMS operators, allowing them to quickly react to changing situations and to easily view video of past events and filter them by gender, age or person ID.

"SentiVeillance Server enables advanced analytics in many video management systems where it was too complex or too expensive before," said Aurimas Juska, Neurotechnology software development team lead. "Users can benefit from an enhanced surveillance system with only a small amount of configuration and no need for programming."

SentiVeillance Server supports most popular video management systems: Milestone XProtect VMS and Luxriot Evo, Evo S and Evo Global. SentiVeillance Server can process up to 10 video streams from multiple video management systems, all in real time.

SentiVeillance Server includes Neurotechnology's latest deep neural-network-based facial detection and recognition algorithm which significantly improves identification accuracy and speed. The algorithm is based on more than 13 years of development and research and has been tested in the NIST Face Recognition Vendor Test (FRVT) Ongoing. It is also included in other Neurotechnology products, such as the VeriLook and MegaMatcher software development kits (SDK), which have millions of deployments worldwide.

Neurotechnology also offers the SentiVeillance SDK for development of solutions using facial identification and object recognition from surveillance video.

SentiVeillance Server and the SDKs noted above are all available through Neurotechnology or from distributors worldwide.

For more information and trial version, go to: www.neurotechnology.com.

ℹ **REQUEST MORE INFORMATION**

FORENSICS

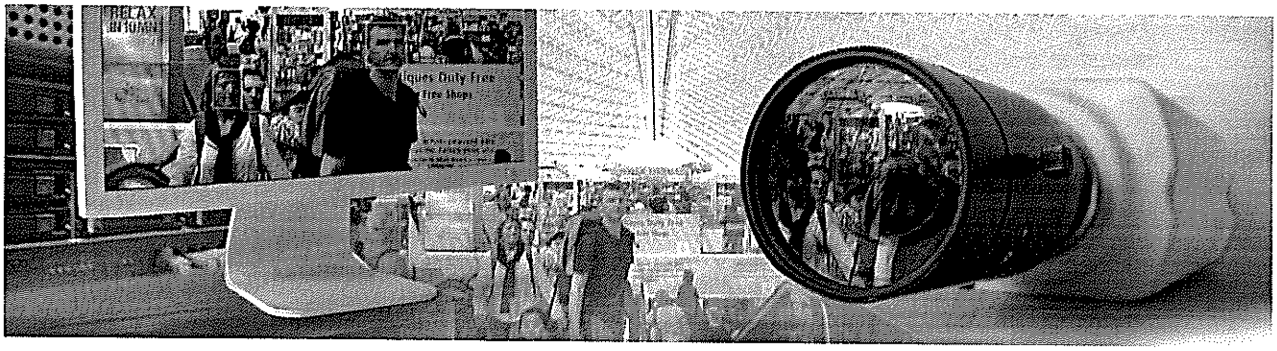
NEUROTECHNOLOGY

Home // Investigations // Forensics // Facial Recognition // SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server uses deep neural network technology to provide facial recognition and tracking capabilities for surveillance video management systems.

NEUROTECHNOLOGY — JUNE 20, 2017



VIEW GALLERY 🖼

SentiVeillance Server is a ready-to-use solution that integrates with surveillance video management systems (VMS). Based on the company's deep neural network technology for facial recognition from surveillance camera video, SentiVeillance Server enhances VMS with advanced capabilities, such as the ability to quickly and accurately recognize faces in video streams and trigger analytical event notifications whenever an authorized, unauthorized or unknown person is detected. This greatly improves the workflow of VMS operators, allowing them to quickly react to changing situations and to easily view video of past events and filter them by gender, age or person ID.

"SentiVeillance Server enables advanced analytics in many video management systems where it was too complex or too expensive before," said Aurimas Juska, Neurotechnology software development team lead. "Users can benefit from an enhanced surveillance system with only a small amount of configuration and no need for programming."

SentiVeillance Server supports most popular video management systems: Milestone XProtect VMS and Luxriot Evo, Evo S and Evo Global. SentiVeillance Server can process up to 10 video streams from multiple video management systems, all in real time.

SentiVeillance Server includes Neurotechnology's latest deep neural-network-based facial detection and recognition algorithm which significantly improves identification accuracy and speed. The algorithm is based on more than 13 years of development and research and has been tested in the NIST Face Recognition Vendor Test (FRVT) Ongoing. It is also included in other Neurotechnology products, such as the VeriLook and MegaMatcher software development kits (SDK), which have millions of deployments worldwide.

Neurotechnology also offers the SentiVeillance SDK for development of solutions using facial identification and object recognition from surveillance video.

SentiVeillance Server and the SDKs noted above are all available through Neurotechnology or from distributors worldwide.

For more information and trial version, go to: www.neurotechnology.com.

ℹ REQUEST MORE INFORMATION

FORENSICS

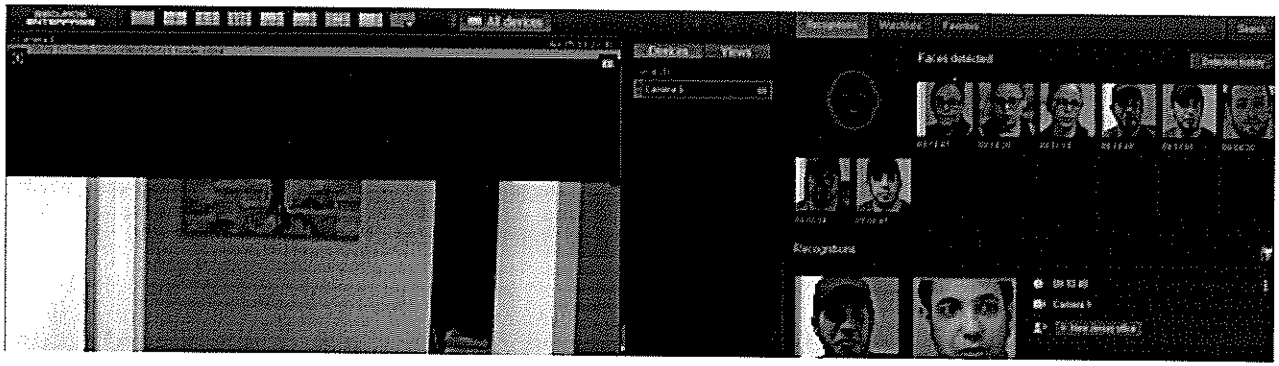
NEUROTECHNOLOGY

Home // Investigations // Forensics // Facial Recognition

Facial Recognition

The Officer.com Facial Recognition product category is a collection of information, product listings and resources for researching various law enforcement Facial Recognition options.

LATEST PRODUCTS



SecurOS FaceX Analytics

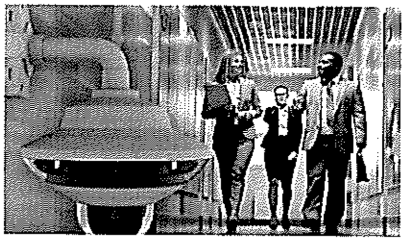
INTELLIGENT SECURITY SYSTEMS (ISS)

FACIAL RECOGNITION APRIL 17, 2019

Safr Facial Recognition Solution

MOC1 SOLUTIONS, A DIVISION OF MOBILE OFFICE COMMUNICATIONS INC.

FACIAL RECOGNITION MARCH 21, 2019



MORE PRODUCTS

Report: NYPD Using Celebrity Photos to Track Down Criminals

When they are stumped for quality images of possible crime suspects, the NYPD sometimes uses celebrity photos to find a match in its facial recognition system, a new report reveals.

FACIAL RECOGNITION MAY 17, 2019

San Francisco Lawmakers Ban Facial Recognition for Police

The legislation also will force police to disclose what surveillance technology they currently use and seek approval on any new technology that either collects or stores someone's data.

FACIAL RECOGNITION MAY 16, 2019

IDentyTech Solutions Ltd.

SECURITY & SURVEILLANCE FEB. 5, 2019

BriefCam Announces Real-Time Face Recognition for Enhanced Situational Awareness

BRIEFCAM

BriefCam's Comprehensive Video Content Analytics Platform Raises the Bar with New Breakthrough Capabilities, Precise Accuracy and Superior Performance

FACIAL RECOGNITION NOV. 14, 2018

Product News: 18 Products for Homeland Defense & Security

New products in anti-terrorism, event security, surveillance, threat detection, and more.

SECURITY & SURVEILLANCE OCT. 3, 2018

Panasonic Showcases Unified Digital Evidence, Body Worn, In Car Video and More at IACP 2018

PANASONIC SYSTEM COMMUNICATIONS CO. OF NORTH AMERICA

EVIDENCE & FORENSIC SOFTWARE OCT. 7, 2018

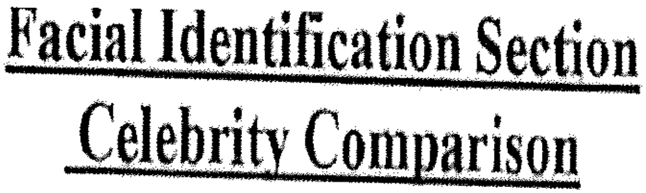
Home // Investigations // Forensics // Facial Recognition // Report: NYPD Using Celebrity Photos to Track Down Criminals

Report: NYPD Using Celebrity Photos to Track Down Criminals

When they are stumped for quality images of possible crime suspects, the NYPD sometimes uses celebrity photos to find a match in its facial recognition system, a new report reveals.

BY GRAHAM RAYMAN — MAY 17, 2019

SOURCE: NEW YORK DAILY NEWS



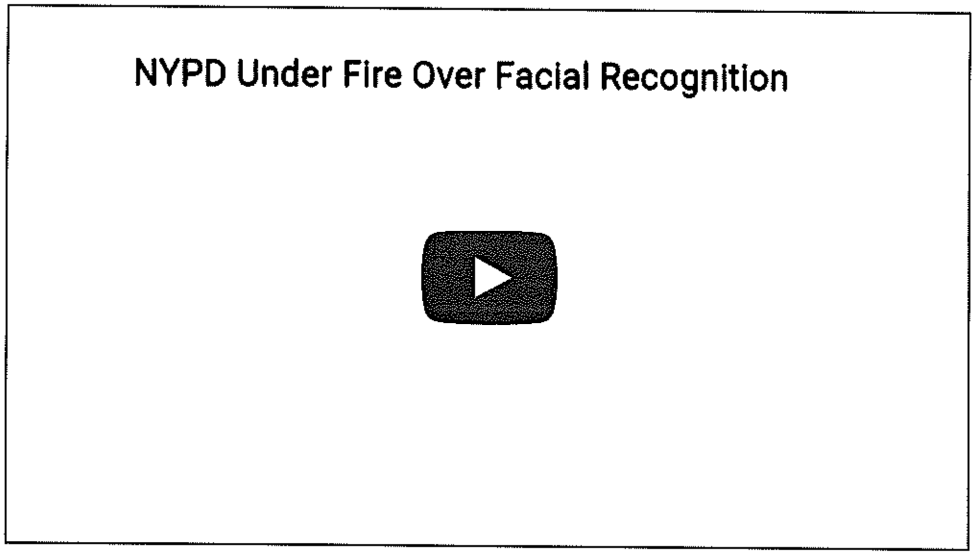
Facial Identification Section

Celebrity Comparison

This undated image provided by Georgetown University's Center on Privacy and Technology shows presentation material with images of a wanted suspect in a New York Police Department document obtained by the university. Georgetown University's Center on Privacy and Technology published a report Thursday, May 16, 2019, on what it says are flawed practices in law enforcement's use of facial recognition. The report says NYPD used a photo of Woody Harrelson in its facial recognition program in an attempt to identify the beer thief who looked like the actor.

GEORGETOWN UNIVERSITY CENTER ON PRIVACY AND TECHNOLOGY

NEW YORK -- When they are stumped for quality images of possible crime suspects, the NYPD sometimes uses celebrity photos to find a match in its facial recognition system, a new report reveals.



NYPD Under Fire Over Facial Recognition

Actor Woody Harrelson's image was used to try to find a match to a man with similar features who stole beer from a pharmacy on April 28, 2017, according to a study by the Georgetown University Center of Privacy and Technology released Thursday.

The thief was caught on store surveillance video, but the images were too blurry to match. A detective decided the suspect looked like Harrelson, so they ran his photo through the database. In another instance, the NYPD used a picture of a New York Knicks player to identify a man wanted for assault in Brooklyn.

The shoplifting case ended with an arrest, but the authors of the report say the NYPD and other police departments too often blur the line of what is ethical when using the facial recognition software.

"There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads," the report said. "(But) The stakes are too high in criminal investigations to rely on unreliable — or wrong — inputs. Unfortunately, police departments' reliance on questionable probe photos appears all too common."

The NYPD's analysts routinely edit photos, sometimes adding in different facial features from other pictures. They "enhances" the images in a way that goes beyond lighting adjustments and color correction, the report said.

Among the things the department changes are facial expressions, opening and closing eyes and mouths - which can look like mug shots, the study said.

"These techniques amount to the fabrication of facial identity points: at best an attempt to create information that isn't there in the first place and at worst introducing evidence that matches someone other than the person being searched for," the report said.

While NYPD guidelines say that any matches are just unconfirmed possible matches, in practice the department has used face recognition matches to place people in lineups. Cops in Jacksonville, Florida and Washington, D.C. similarly used the software. But on Tuesday, San Francisco banned use of the technology.

The NYPD has made 2,878 busts using facial recognition in some manner, according to the report.

"We cannot sit idly while police recklessly expand the use of Orwellian surveillance technologies like face recognition to secretly track people in real-time as they go about their daily lives," said Abdullah Hasan, a spokesman for the American Civil Liberties Union. "This is particularly true for police jurisdictions with troubling histories of discriminatory practices."

In a lengthy statement, the NYPD defended the program, calling a match "merely a lead and not probable cause to arrest."

"The NYPD has been deliberate and responsible in its use of facial recognition technology," the department said. "We do not engage in mass or random collection of facial records from NYPD camera systems, the internet, or social media."

Police credit the software for assisting in the arrest of a man for throwing urine at MTA conductors, the bust of a man who pushed a straphanger on to the subway tracks, and a successful missing persons case involving a woman with Alzheimer's.

"The leads generated have also led to arrests for homicides, rapes and robberies," the department said. "The NYPD constantly reassesses our existing procedures and in line with that are in the process of reviewing our existent facial recognition protocols."

———

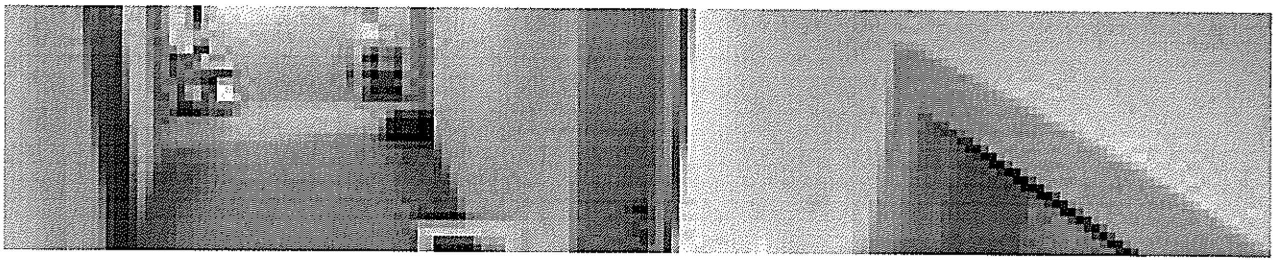
Visit New York Daily News at www.nydailynews.com

Distributed by Tribune Content Agency, LLC.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?



FACIAL RECOGNITION

San Francisco Becomes First to Ban Use of Facial Recognition Technology by Police

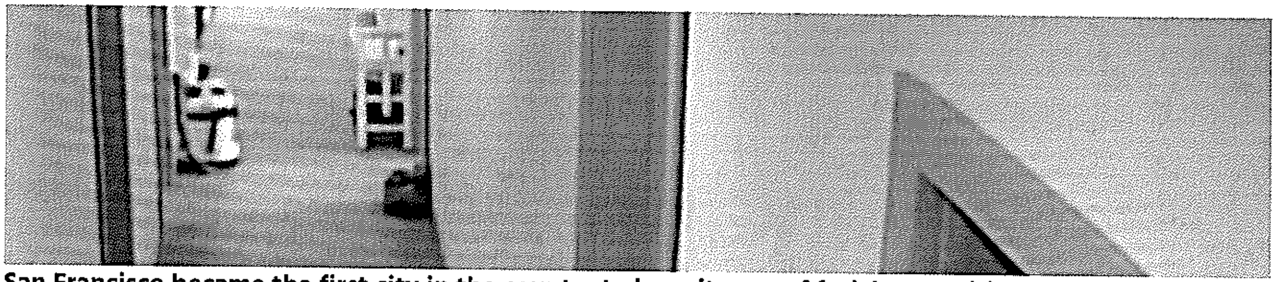
Home // Investigations // Forensics // Facial Recognition // San Francisco Becomes First to Ban Use of Facial Recognition Technology by Police

San Francisco Becomes First to Ban Use of Facial Recognition Technology by Police

The legislation also will force police to disclose what surveillance technology they currently use and seek approval on any new technology that either collects or stores someone's data.

BY TRISHA THADANI — MAY 16, 2019

SOURCE: SAN FRANCISCO CHRONICLE



San Francisco became the first city in the country to ban city use of facial recognition surveillance technology Tuesday -- a groundbreaking move that privacy advocates applaud, but others say may go too far.
AMAZON

SAN FRANCISCO -- San Francisco became the first city in the country to ban city use of facial recognition surveillance technology Tuesday — a groundbreaking move that privacy advocates applaud, but others say may go too far.

The legislation, written by Supervisor Aaron Peskin, also will force city departments to disclose what surveillance technology they currently use — and seek approval from the Board of Supervisors on any new technology that either collects or stores someone's data.

"This is really about saying we can have security without being a security state. We can have good policing without being a police state," Peskin said at Tuesday's board meeting. "Part of that is building trust with the community."

The ordinance passed the board 8-1, with Supervisor Catherine Stefani the dissenter. Supervisors Hillary Ronen and Shamann Walton were absent. The board must vote on the ordinance one more time before it officially passes and moves to Mayor London Breed for a signature.

Stefani said she was concerned about how a complete ban on facial recognition could prevent the city's law enforcement from having access to a potentially useful crime-solving tool. She also worried that forcing departments to disclose all their surveillance technology — and requiring them to seekboard approval on anything new — could bog them down with extra work.

"I am not yet convinced, and I still have many outstanding questions," she said. But "that does not undermine what I think is a very well-intentioned piece of legislation."

The San Francisco Police Department estimated it would take between two and four full-time employees to comply with the new ordinance. And even though the department says it does not currently use facial recognition technology, it may no longer acquire it in the future.

The airport and port would be exempt from the ban, as they are federally regulated.

Local advocacy group Stop Crime SF said the city should have considered a moratorium on the technology, rather than an outright ban.

"We agree there are problems with facial recognition ID technology and it should not be used today," Joel Engardio, the group's vice president said in a statement. "But the technology will improve and it could be a useful tool for public safety when used responsibly and with greater accuracy. We should keep the door open for that possibility."

While facial recognition is becoming increasingly common, it is still expensive and has been blamed for major inaccuracies, particularly when identifying minorities. Those who support the ban say it is important for the city to rein in the emerging technology, which is largely unregulated in the United States.

San Francisco is not the only city that has considered a ban. The Oakland City Council may vote on a similar measure later this year, while city officials in Somerville, Mass., recently began discussing a similar ban.

"With all the changes in tech that we may not understand today, it is important to bring its use to light, while balancing the need for public safety," Supervisor Ahsha Safai said.

Trisha Thadani is a San Francisco Chronicle staff writer.
Email: tthadani@sfchronicle.com Twtter: @TrishaThadani

———

Visit the San Francisco Chronicle at www.sfchronicle.com

Distributed by Tribune Content Agency, LLC.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

Posted ByLAHeat May 16 2019 17:47

Hey, I have an idea! Let's ban running license plates for wants and warrants, and let's ban running suspect's finger prints, and AFIS, and let's ban DNA, and, what the heck, ban the police while we are at it! Then the politicians will have what they want! Then the politicians can police the damn city- since they know better than anyone else!

FACIAL RECOGNITION

Report: NYPD Using Celebrity Photos to Track Down Criminals

Home // Investigations // Forensics // Facial Recognition // SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server - Face Recognition and Analytics to Video Management Systems

SentiVeillance Server uses deep neural network technology to provide facial recognition and tracking capabilities for surveillance video management systems.

NEUROTECHNOLOGY — JUNE 20, 2017

VIEW GALLERY

SentiVeillance Server is a ready-to-use solution that integrates with surveillance video management systems (VMS). Based on the company's deep neural network technology for facial recognition from surveillance camera video, SentiVeillance Server enhances VMS with advanced capabilities, such as the ability to quickly and accurately recognize faces in video streams and trigger analytical event notifications whenever an authorized, unauthorized or unknown person is detected. This greatly improves the workflow of VMS operators, allowing them to quickly react to changing situations and to easily view video of past events and filter them by gender, age or person ID.

"SentiVeillance Server enables advanced analytics in many video management systems where it was too complex or too expensive before," said Aurimas Juska, Neurotechnology software development team lead. "Users can benefit from an enhanced surveillance system with only a small amount of configuration and no need for programming."

SentiVeillance Server supports most popular video management systems: Milestone XProtect VMS and Luxriot Evo, Evo S and Evo Global. SentiVeillance Server can process up to 10 video streams from multiple video management systems, all in real time.

SentiVeillance Server includes Neurotechnology's latest deep neural-network-based facial detection and recognition algorithm which significantly improves identification accuracy and speed. The algorithm is based on more than 13 years of development and research and has been tested in the NIST Face Recognition Vendor Test (FRVT) Ongoing. It is also included in other Neurotechnology products, such as the VeriLook and MegaMatcher software development kits (SDK), which have millions of deployments worldwide.

Neurotechnology also offers the SentiVeillance SDK for development of solutions using facial identification and object recognition from surveillance video.

SentiVeillance Server and the SDKs noted above are all available through Neurotechnology or from distributors worldwide.

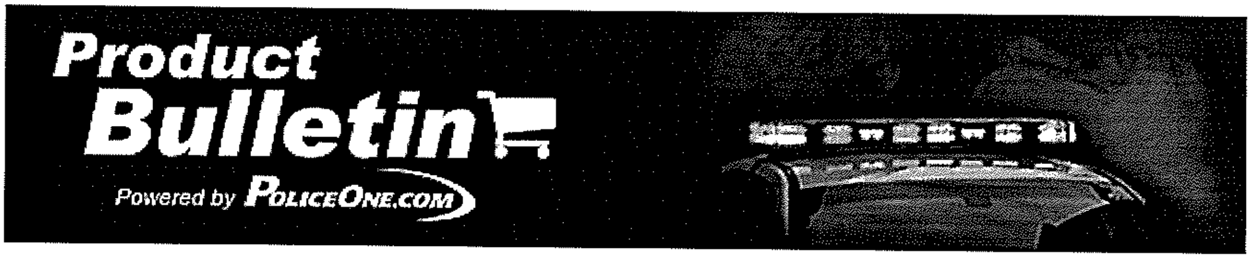
For more information and trial version, go to: www.neurotechnology.com.

REQUEST MORE INFORMATION

FORENSICS

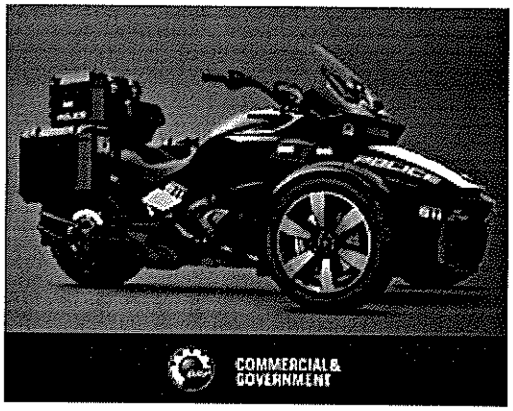
NEUROTECHNOLOGY

June 22, 2017 | View as webpage



Download the Mobile App

Police Performance with Peace-of-Mind



We took the stability and performance of our Spyder 3-Wheeler and added the features that today's officers need to get the job done.

Request a quote >

Investigative Platform Helps Solve Major Crimes

VIGILANT SOLUTIONS

Develop leads, solve crimes and protect officers with license plate recognition (LPR), analytics and facial recognition from Vigilant Solutions.

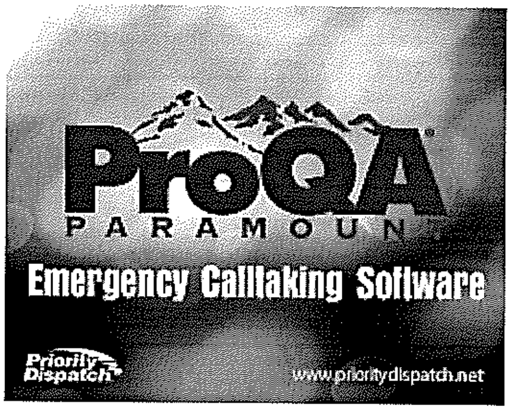
Download the eBook >

Pack More Protection with Dual-Strike Face Rifle Plates

ProQA Dispatching is Faster Dispatching

Stack two Angel Armor Truth SNAP magnetic plates together to protect against NIJ Level IIIA and Level III threats, including AK-47, 5.56 and .308.

Get armored now! >



Find out how the latest upgrades to ProQA for Police make dispatching faster and even more accurate.

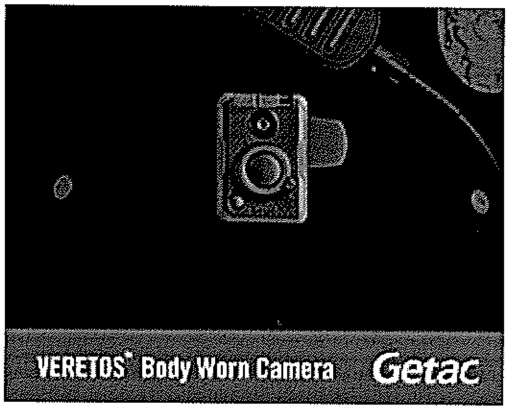
See it in action >

IR Patrol M250XR Extended Range Thermal Imager

Designed to fill the need for long range thermal detection the new IR Patrol XR makes an ideal companion for any after dark surveillance application.

Learn more at Aurora Tactical >

Getac Veretos Body Worn Camera

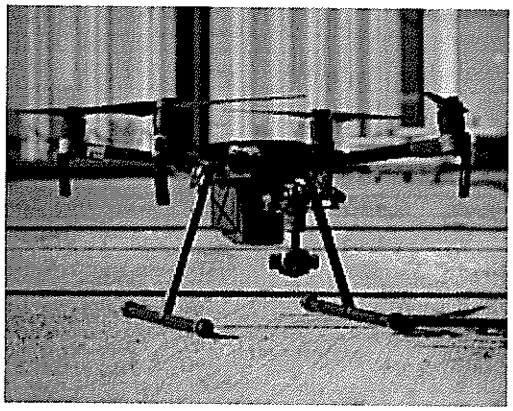


With a compact, rugged design, full HD video, and 12 hours of battery, the Getac Veretos delivers complete situational awareness in critical scenarios.

Learn more >

Perform Large-Scale Operations Without Putting Officers at Risk

When There's Action, There's Quick Reaction



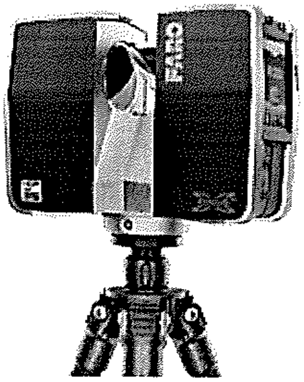
UAV imaging drones are invaluable for surveying large areas, finding suspects or victims, assessing crime and accident scenes, searching for missing persons and many other emergency responses.

Contact us for an LEO discount >

When seconds count, you have time to spare. The new Quick Reaction Force Series from Tactical Research is ready when you are... Before, actually.

Learn more about our boots >

Fast and Accurate Focus3D Laser Scanner from FARO



Laser Scanners designed for fast and exact indoor and outdoor three-dimensional documentation: Simplicity at your fingertips.

Learn more and request a demo >

Get Free Grant Help for a New Mobile Command Center

LDV has partnered with PoliceOne's grant experts to get the funding your department needs for a mobile command center or emergency vehicle.

Contact our grant experts >

There is Only One PRO

Still Spillman.

With extreme durability and a budget friendly price, the Aimpoint PRO is the best choice for LE. Accept no substitute.

Complete and ready to mount >

spillman®
technologies, inc.

Spillman Technologies has been a trusted source in public safety technology for over 30 years.

Why we're still an industry leader >

BLUtube POWERED BY POLICEONE.COM

POLICEONE.COM ACADEMY

PoliceGrantsHelp.com

This message was sent to mallard@northamptonma.gov from:

P1 Product Bulletin | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

PoliceOne.com

Topics > 2017 Guide to Emerging Technologies > Articles

Cop Gumbo

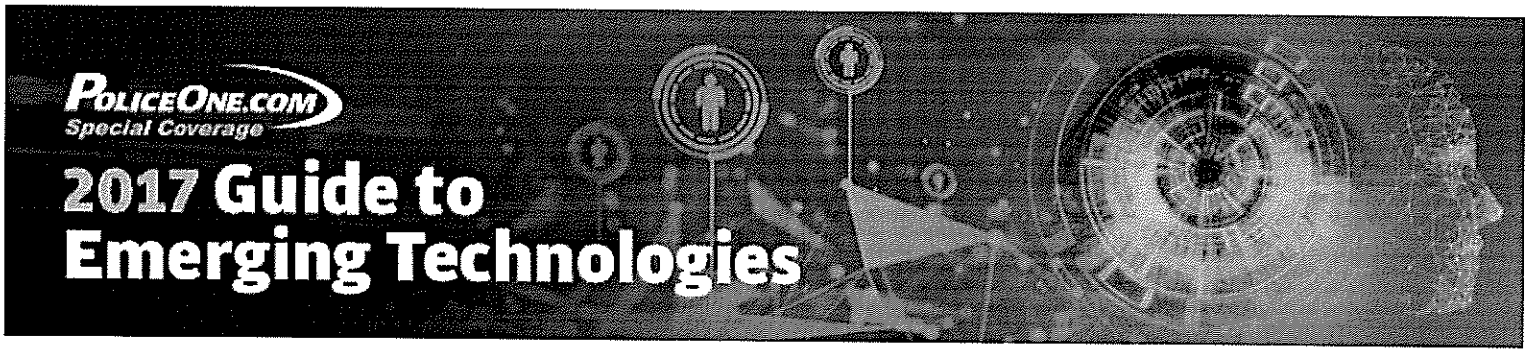
with Val Van Brocklin

Facial recognition technology and a 'reasonable expectation of privacy'

Law enforcement might consider using discretion before a court decides whether police need a warrant to scan someone's face

Editor's Note:

From crafting policy to tactical considerations, PoliceOne's **2017 Guide to Emerging Technologies** features expert analysis on soundwave technology, facial recognition software, handheld narcotics analyzers, the future of traffic stops, how constitutional law impacts the collection of data for investigations, and how advancements in biometric technologies will help improve correctional facilities.



Sept. 11 demonstrated that the greatest military might in the world couldn't protect us against the "asymmetric threats" of a few "unidentifiable enemies." The idea that FRT could identify terrorist suspects in public locations before they committed their crimes seemed to offer some protection.

Last May, the Government Accountability Office (GAO) issued a report about the FBI's amassing of 411.9 million facial images as part of its Next Generation Identification (NGI) program. It criticized the

program's secrecy and intrusion on privacy. Eighty percent of the photos were of people who had committed no crime. That's a significant police-created biometric database of primarily law-abiding Americans.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available. (Photo/Pixabay)

"If you're reading this in the United States, there's a 50 percent chance that a photo of your face is in at least one database used in police facial-recognition systems," reported the Atlantic Monthly last October.

Georgetown Law's Center for Privacy and Technology published a report the same month addressing the scale of local and state police involvement in facial recognition. The year-long investigation was based on more than 15,000 pages of records obtained through more than 100 FOIA requests. It found that police departments in nearly half the states can use facial-recognition software to compare surveillance images with databases of ID photos or mugshots. Some departments only use the technology to confirm the identity of a suspect who's been detained; others continuously analyze footage from surveillance cameras.

The GAO and Georgetown Law's reports are fueling public debate, which often lags behind evolving technology – as do court decisions. To date, I could find no court ruling on police use of FRT and the Fourth Amendment's reasonable expectation of privacy against government intrusion absent probable cause and a warrant.

PUBLIC DEBATE

Proponents of police use of FRT argue:

- There is no expectation of privacy to your face once you take it out in public.

- Any privacy intrusion is a small price to pay for increased public safety.

- What difference does it make if the government has a digital algorithm of your face they can use to ID you if you haven't done – or aren't doing – anything wrong?

Privacy advocates' concerns include:

- A reasonable expectation of privacy includes a reasonable expectation of anonymity from government use of computer algorithms and databases to capture law abiding citizens' faces and identify them without their knowledge or consent.

- FRT allows for a different kind of tracking that can occur from far away, in secret, and on large numbers of people. Fingerprints are only left on things you touch and you know when police are taking them. You can't leave your face at home and, with limited exceptions, it isn't acceptable to cover it. Depending how it's used, FRT could rob citizens of a reasonable expectation of anonymity.

Giving police the rights to do this without judicial oversight creates a slippery slope that could lead to real-time, mass surveillance like that of Big Brother. Police have an incentive to collect as many photos as possible because the larger the database the more likely they are to get a match and solve a crime or identify a suspect or person of interest.

- Real-time, mass surveillance could also chill First Amendment speech unpopular with the government. Advocates point to the FBI's disgraced COINTELPRO program of surveillance against civil rights activists and Vietnam War protesters during the '60s and '70s.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available.

LEGAL QUESTIONS

While the courts have not yet addressed the following, they will. Law enforcement would serve itself well not to go into those cases with a record of overreaching, else the courts restrain us more than we might have effectively restrained ourselves.

1. Does a face recognition constitute a "search" that triggers Fourth Amendment protection?

2. What is the legal standard police must meet before using FRT?

3. Does your state have a law regulating the collection of biometric data?

4. Do your state courts offer more protection against government intrusion under your state constitution than the Supreme Court does under the U.S. Constitution? See, for example, an analysis of FRT under Utah case law as distinguished from the same analysis under federal case law.

PLAN AND CONSIDER

1. Consulting with your prosecutor about federal and state laws and court cases that might be relevant to police use of FRT.

2. Adopting FRT use policies and making them public. Here is a sample policy.

3. Training officers to ensure the most effective use of the scanners. The Institute of Electrical and Electronics Engineers (IEEE) Certified Biometrics Professional (CBP) program offers courses which set a baseline of biometric knowledge for those who plan to use FRT. These course standards aren't yet national but some agencies have adopted them as certification standards.

Law-abiding citizens are not against police use of FRT. Georgetown Law's Center on Privacy & Technology noted:

> *The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of*

> *good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.*

But the public has real concerns about FRT and privacy. Concerns we'd do well to consider in advance of court rulings.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags > Investigations • Legal • Warrants

POLICEONE.COM

Topics > 2017 Guide to Emerging Technologies > Articles

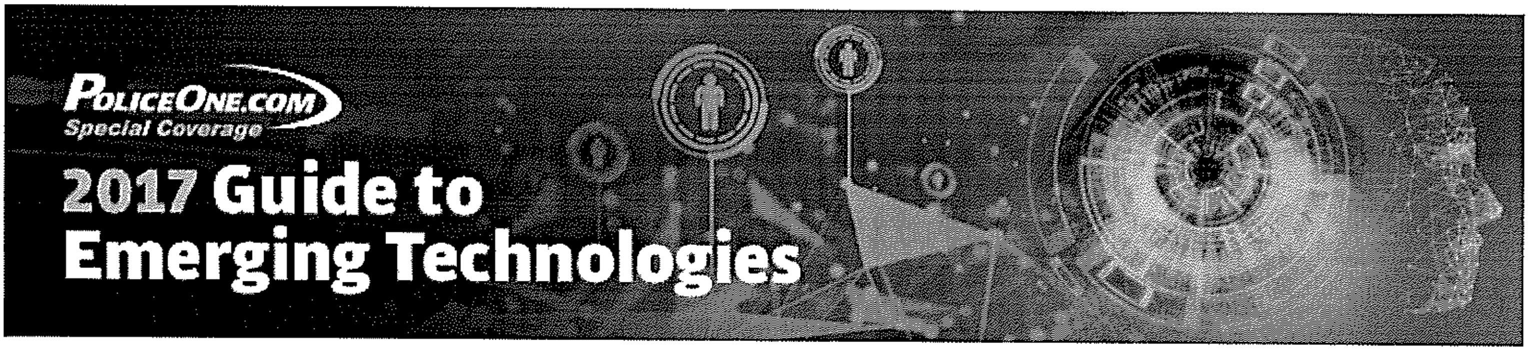
Cop Gumbo
with Val Van Brocklin

Facial recognition technology and a 'reasonable expectation of privacy'

Law enforcement might consider using discretion before a court decides whether police need a warrant to scan someone's face

Editor's Note:

From crafting policy to tactical considerations, PoliceOne's **2017 Guide to Emerging Technologies** features expert analysis on soundwave technology, facial recognition software, handheld narcotics analyzers, the future of traffic stops, how constitutional law impacts the collection of data for investigations, and how advancements in biometric technologies will help improve correctional facilities.



Sept. 11 demonstrated that the greatest military might in the world couldn't protect us against the "asymmetric threats" of a few "unidentifiable enemies." The idea that FRT could identify terrorist suspects in public locations before they committed their crimes seemed to offer some protection.

Last May, the Government Accountability Office (GAO) issued a report about the FBI's amassing of 411.9 million facial images as part of its Next Generation Identification (NGI) program. It criticized the

program's secrecy and intrusion on privacy. Eighty percent of the photos were of people who had committed no crime. That's a significant police-created biometric database of primarily law-abiding Americans.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available. (Photo/Pixabay)

"If you're reading this in the United States, there's a 50 percent chance that a photo of your face is in at least one database used in police facial-recognition systems," reported the Atlantic Monthly last October.

Georgetown Law's Center for Privacy and Technology published a report the same month addressing the scale of local and state police involvement in facial recognition. The year-long investigation was based on more than 15,000 pages of records obtained through more than 100 FOIA requests. It found that police departments in nearly half the states can use facial-recognition software to compare surveillance images with databases of ID photos or mugshots. Some departments only use the technology to confirm the identity of a suspect who's been detained; others continuously analyze footage from surveillance cameras.

The GAO and Georgetown Law's reports are fueling public debate, which often lags behind evolving technology – as do court decisions. To date, I could find no court ruling on police use of FRT and the Fourth Amendment's reasonable expectation of privacy against government intrusion absent probable cause and a warrant.

PUBLIC DEBATE

Proponents of police use of FRT argue:

- There is no expectation of privacy to your face once you take it out in public.

- Any privacy intrusion is a small price to pay for increased public safety.

- What difference does it make if the government has a digital algorithm of your face they can use to ID you if you haven't done – or aren't doing – anything wrong?

Privacy advocates' concerns include:

- A reasonable expectation of privacy includes a reasonable expectation of anonymity from government use of computer algorithms and databases to capture law abiding citizens' faces and identify them without their knowledge or consent.

- FRT allows for a different kind of tracking that can occur from far away, in secret, and on large numbers of people. Fingerprints are only left on things you touch and you know when police are taking them. You can't leave your face at home and, with limited exceptions, it isn't acceptable to cover it. Depending how it's used, FRT could rob citizens of a reasonable expectation of anonymity.

Giving police the right to do this without judicial oversight creates a slippery slope that could lead to real-time, mass surveillance like that of Big Brother. Police have an incentive to collect as many photos as possible because the larger the database the more likely they are to get a match and solve a crime or identify a suspect or person of interest.

- Real-time, mass surveillance could also chill First Amendment speech unpopular with the government. Advocates point to the FBI's disgraced COINTELPRO program of surveillance against civil rights activists and Vietnam War protesters during the ‘60s and ‘70s.

When debating any privacy compromises associated with FRT and active surveillance, society must weigh the costs associated with forgoing anonymity in public versus the benefit of active crime prevention using the newest technology available.

LEGAL QUESTIONS

While the courts have not yet addressed the following, they will. Law enforcement would serve itself well not to go into those cases with a record of overreaching, else the courts restrain us more than we might have effectively restrained ourselves.

1. Does a face recognition constitute a “search” that triggers Fourth Amendment protection?

2. What is the legal standard police must meet before using FRT?

3. Does your state have a law regulating the collection of biometric data?

4. Do your state courts offer more protection against government intrusion under your state constitution than the Supreme Court does under the U.S. Constitution? See, for example, an analysis of FRT under Utah case law as distinguished from the same analysis under federal case law.

PLAN AND CONSIDER

1. Consulting with your prosecutor about federal and state laws and court cases that might be relevant to police use of FRT.

2. Adopting FRT use policies and making them public. Here is a sample policy.

3. Training officers to ensure the most effective use of the scanners. The Institute of Electrical and Electronics Engineers (IEEE) Certified Biometrics Professional (CBP) program offers courses which set a baseline of biometric knowledge for those who plan to use FRT. These course standards aren't yet national but some agencies have adopted them as certification standards.

Law-abiding citizens are not against police use of FRT. Georgetown Law's Center on Privacy & Technology noted:

> *The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of*

> *good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.*

But the public has real concerns about FRT and privacy. Concerns we'd do well to consider in advance of court rulings.

About the author

As a state and federal prosecutor, Val's trial work was featured on ABC'S PRIMETIME LIVE, Discovery Channel's Justice Files, in USA Today, The National Enquirer and REDBOOK. Described by Calibre Press as "the indisputable master of entertrainment," Val is now an international law enforcement trainer and writer. She's had hundreds of articles published online and in print. She appears in person and on TV, radio, and video productions. When she's not working, Val can be found flying her airplane with her retriever, a shotgun, a fly rod, and high aspirations. Visit Val at www.valvanbrocklin.com and info@valvanbrocklin.com

Tags › Investigations • Legal • Warrants

WEBINAR: FACIAL RECOGNITION AND CYBER CRIMES

May 19th, 3:00 PM EST / 2:00 PM CST

REGISTER NOW

THE THREAT FROM CYBER CRIMES IS SERIOUS – AND GROWING.

And it's not just corporations that are at risk from this threat. Adults and children in your community could be targets of fraudsters, identity thieves, and online predators.

In this webinar Retired NYPD Detective, Roger Rodriguez will share how to analyze images for cyber-crime investigations such as prostitution rings, identity theft, fraud, and child exploitation using poor quality images obtained from crime victims, social media, or other online sources.

REGISTER NOW

*Must use valid Law Enforcement Agency email address to register

2021 Las Positas Ct, Suite #101 Livermore, CA 94551

Vigilant Solutions

If you are having trouble viewing, please click here.

This e-mail is being sent to mallard@northamptonma.gov.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Change E-mail | Forward to a Friend | Customer Service Center | Privacy Policy

If this e-mail was forwarded to you and you are interested in subscribing to our emails, please click here to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer.com
SouthComm Business Media, LLC
1233 Janesville Ave
Fort Atkinson, WI 53538

This rough transcript is an interview conducted by Jessica Berger, MLIS candidate from SJSU with Northampton MA Police Captain Cartledge and Officer Allard, who generously donated their time to help with the foregoing research project about drones.

Text in brackets ( ) indicate either added words to clarify - or to note where the audio was unclear and caused some confusion during the transcription process.

How did you get started working with drones?
Drones in our industry have become a little more popular as far as search and rescue tools and investigative tools. You think of deploying a helicopter from an hour and a half away at thousands and thousands of dollars and then the ability to get a more inexpensive way to actually look for people- we get a lot of missing people who are victims in the woods... (We try to look for) the best investigative (methods). (Using drones we can) find lost people, (take) aerial photos of accidents, find evidence you can't find from the road. We assist the DPW with vegetation loss and help firefighters (by) giving them an aerial view.

(The drone program) started in January (of 2017?) we came up with a lot of research, policies, procedures and (obtained) approval from the government.

I'm an FAA licensed pilot and Seargeant Moody is licensed. This has been used throughout the (country). You get to see what an impressive tool this is.

(When using drones) we're coming from a 12 minute deployment - if we are on duty. So it's a quicker deployment than waiting for the State Police, which could take hours depending on the weather.

What about kidnapping?
It's hard to say with particular cases. We don't have FLIR, (which is) thermal imaging.

(With FLIR) You will see a body signature if you have someone in the woods (which otherwise) would be hard to see through the trees. But with thermal imaging you can see people lost in the woods

What are some of the drone initiatives right now?
We are currently working with the DPW (The Department of Public Works) doing aerial shots for them in areas they are concerned with and used (these aerial shots taken by drones) on crime scenes; a lot of training flights; one of them is marshland they have problems with beavers. You can't walk out there to get an aerial view of the beaver dam.

About obtaining drones:

Must be registered if over 0.55 lbs.

Can you explain the data collection policies?
All digital media evidence (DME) policy regulates that and audit procedures all strictly written digital media all video and images, we have policies that I may have a policy in A that derives for policy in B- they work together.

Do police use drones equipped with facial recognition apps?

A: No, these are not equipped (with facial recognition apps) in the police industry. You will not see that in law enforcement

J: I think for people with privacy concerns that is a big reassurance

Our drone doesn't have that (facial recognition) capability and under the guides of police association, that is clearly spelled out.

The records management (department provides) the policies I already talked to you about. All the policies are on the website and the new public records law changed recently and I'm not sure how that impacts the digital requests from the people
Someone sends or denies it.

Do you have an opinion about legislative changes that should be made regarding drones?
I would not personally say thoughts on rules but all pilots should abide by the FAA regulations. The FAA came up with (new) ones in Aug 2016 and March 2017 they are very informative and strict enough. There wouldn't be anything I would change; you will see them get stricter. The FAA has a piloting command that (the drone) has to be piloted for police or someone under direct control by the pilot.
(For hobbyists) all you have to do is register the drone you don't need a pilot license,. You just have to register the drone but you have to abide by the regulations (about) air space, flying over people, everything that is in the regulations- or be fined.

What if people don't abide - will there be people not abiding by regulations, not police, but citizens, in the same way automobile drivers break rules?
You will always have that but in our agency we haven't run across anyone to report to the FAA. So if someone is flying over a crowd, we report them to the FAA and they could be fined. That is not within (our) domain, we are agents of the federal government so we report to them.

How do you identify them?
You identify by asking, when you register a drone whether you have 1 or 10 you have a number put on a drone, the FAA looks at the number and then identifies it (correlates the number of the drone) to the person because it's a registered aircraft.

600,000 drones are predicted to be purchased this year, how might it affect your workload?
A: I don't think it will affect our workload, but it will (impact) the government's, and they will be restricting (drone policy more strictly). They are coming up with technology that aircraft can id drones - and something that will allow aircraft to id drones.

What is your opinion about criminals hacking Smartphones ?
A: The drones aren't Bluetooth enabled, I can't comment
(Our) drone doesn't have that capability. (Ours use) wifi from the remote to the drone and tablet they are using (on the ground). People are coming out with ways to hack drones and take over the phones. But we have the federal government and large corporations being hacked. What's the focus of your paper?

J: Drones as an information security tool because they are up and coming.

Are we the only police dept you are talking to?

As far as I know but wanted to talk to a programmer and the military.

Do you have an opinion about Sky grabber hacking the US military drones that could interfere with a mission. It is a 26 dollar software.
A: I have no idea. (Note- I will leave this out)

They show me the drone.
This is the phantom 4 DJI is the company this is the one we just got; there are different models and prices. This whole set up cost about 1200 dollars - not that expensive – operated gimble system as you fly you move the camera up and down it will do stills and video and it communicates to the remote to the tablet the video what's sent isn't always great. There's an sd card.

Q: To become airborne – how can it take off and stay aloft?
Captain Cartledge and Officer Allard show that the propellers are detached from the craft, which is why at first it looks impossible for it to take off...
A: The computer system is incredible, (there are) top and bottom sonars - it knows its latitude and longitude and where it is; if we lose a signal it will return to where it took off. It knows its GPS position - it wouldn't give us the victim's GPS but would allow us to id that person's place and its flow in direct eyesight. We always know where it is based on the line of site - we have to keep it in our line of sight at all times.

Some of the smaller ones called the Mavic pro foldable can go 3 miles but the FAA still says you need to maintain line of sight.

Every time we fly we have 2 people -we have a pilot in command and a visual observer relaying to the pilot if there are any hazards or harm. If (there is a traffic) accident (we) can stay away but just view (it) from the outskirts. From the tree line we don't have to be right on top -we are standing still from the line of sight. It is pretty strictly regulated.

Q: Are you experimenting with any other technology tools?
A: In general we are a pretty progressive department. We have a lot of other things other agencies have done. We have in-housie AFIS fingerprint systems; we have a ton of things -we have criminal investigation tools others don't have. Our website is informative, but we don't put out everything about our tools (such as the most up to date ones used at a crime scene. (We have) UTD LIDAR (light detection and ranging) – (it is) light detection (in lieu of radar?) We're always looking ahead at tech and it is expensive to (keep up).

Q: Exploring preparations for acquiring drones.
We did it the right way (the preparation for drones). We're an accredited agency - we have policies for everything -we crafted drone policy before we went forward and before we even bought the drone. We try to do things the right way.

J offers to give transcript and asks about the transcript being on the web
Obtains spelling: Allard. Do not use my name

What's the time frame on the paper- I'd like to read it just for my own, send it before you (submit it to your teacher).

Do you want to not have your names in there?

You are the pilot I don't care. When you write this make it clear that all we are doing are under the jurisdiction of the FAA, get it to us before deadline and we can change it I don't want to jeopardize license.

On Sat, Apr 15, 2017 at 6:34 AM, John Cartledge <jcartledge@northamptonma.gov> wrote:

> Mike... let me know what u think...
>
> ***Captain John D. Cartledge***
> ***Operations Division Commander***
> *Northampton Police Department*
> *29 Center St*
> *Northampton, MA 01060*
> *413-587-1100(Dispatch)*
> *413-587-1176(Office)*
> *413-587-1137(Fax)*
> *www.northamptonpd.com*
>
> Begin forwarded message:
>
> **From:** Jessica Berger <jsberger@outlook.com>
> **Date:** April 14, 2017 at 16:11:48 EDT
> **To:** "jcartledge@northamptonma.gov" <jcartledge@northamptonma.gov>
> **Subject: Transcript**
>
> Dear Captain Cartledge,
>
> Thank you and Officer Allard for so generously donating your time today. It will go a long way towards improving my research.
> Below is the rough transcript. Feel free to make edits anywhere you deem appropriate. The highlighted area in particular would benefit from attention.
> I will keep you updated about the final project and make sure to incorporate your changes.
>
> Thank you again. Have a good Easter.
>
> Respectfully,
> Jessica Berger
>
> This rough transcript is an interview conducted by Jessica Berger, MLIS candidate from SJSU with Northampton MA Police Captain Cartledge and Officer Allard, who generously donated their time to help with the foregoing research project about drones.
>
> Text in brackets ( ) indicate either added words to clarify - or to note where the audio was unclear and caused some confusion during the transcription process.
>
> *How did you get started working with drones?*

Drones in our industry have become a little more popular as far as search and rescue tools and investigative tools. You think of deploying a helicopter from an hour and a half away at thousands and thousands of dollars and then the ability to get a more inexpensive way to actually look for people- we get a lot of missing people who are victims in the woods... (We try to look for) the best investigative (methods). (Using drones we can) find lost people, (take) aerial photos of accidents, find evidence you can't find from the road. We assist the DPW with vegetation loss and help firefighters (by) giving them an aerial view.

(The drone program) started in January (of 2017?) we came up with a lot of research, policies, procedures and (obtained) approval from the government.

I'm an FAA licensed pilot and Seargeant Moody is licensed. This has been used throughout the (country). You get to see what an impressive tool this is.

(When using drones) we're coming from a 12 minute deployment - if we are on duty. So it's a quicker deployment than waiting for the State Police, which could take hours depending on the weather.

What about kidnapping?
It's hard to say with particular cases. We don't have FLIR, (which is) thermal imaging.

(With FLIR) You will see a body signature if you have someone in the woods (which otherwise) would be hard to see through the trees. But with thermal imaging you can see people lost in the woods

What are some of the drone initiatives right now?
We are currently working with the DPW (The Department of Public Works) doing aerial shots for them in areas they are concerned with and used (these aerial shots taken by drones) on crime scenes; a lot of training flights; one of them is marshland they have problems with beavers. You can't walk out there to get an aerial view of the beaver dam.

About obtaining drones:
(???Anyone well cit. can buy drones over age 13 register if the weight of the drone 5.5. or higher all have to be registered with FAA all regulations are posted there.
???FAA part 107 governs how drones are operated, which need registered???)

Can you explain the data collection policies?
All digital media evidence (DME) policy regulates that and audit procedures all strictly written digital media all video and images, we have policies that I may have a policy in A that derives for policy in B- they work together.

Do police use drones equipped with facial recognition apps?
A: No, these are not equipped (with facial recognition apps) in the police industry. You will not see that in law enforcement

J: I think for people with privacy concerns that is a big reassurance

Our drone doesn't have that (facial recognition) capability and under the guides of police association, that is clearly spelled out.

The records management (department provides) the policies I already talked to you about. All the policies are on the website and the new public records law changed recently and I'm not sure how that impacts the digital requests from the people Someone sends or denies it.

Do you have an opinion about legislative changes that should be made regarding drones?
I would not personally say thoughts on rules but all pilots should abide by the FAA regulations. The FAA came up with (new) ones in Aug 2016 and March 2017 they are very informative and strict enough. There wouldn't be anything I would change; you will see them get stricter. The FAA has a piloting command that (the drone) has to be piloted for police or someone under direct control by the pilot.
(For hobbyists) all you have to do is register the drone you don't need a pilot liscense, you have to take a certification exam. You just have to register the drone but you have to abide by the regulations (about) air space, flying over people, everything that is in the regulations- or be fined.

What if people don't abide - will there be people not abiding by regulations, not police, but citizens, in the same way automobile drivers break rules?
You will always have that but in our agency we haven't run across anyone to report to the FAA. So if someone is flying over a crowd, we report them to the FAA and they get fined. That is not within (our) domain, we are agents of the federal government so we report to them.

How do you identify them?
You identify by asking, when you register a drone whether you have 1 or 10 you have a number put on a drone, the FAA looks at the number and then identifies it (correlates the number of the drone) to the person because it's a registered aircraft.

600,000 drones are predicted to be purchased this year, how might it affect your workload?
A: I don't think it will affect our workload, but it will (impact) the government's, and they will be restricting (drone policy more strictly). They are coming up with technology that aircraft can id drones - and something that will allow aircraft to id drones.

What is your opinion about criminals hacking Smartphones ?
A: The drones aren't Bluetooth enabled, I can't comment
(Our) drone doesn't have that capability. (Ours use) wifi from the remote to the drone and tablet they are using (on the ground). People are coming out with ways to hack drones and take over the phones. But we have the federal government and large corporations being hacked. What's the focus of your paper?

J: Drones as an information security tool because they are up and coming.

Are we the only police dept you are talking to?

As far as I know but wanted to talk to a programmer and the military.

Do you have an opinion about Sky grabber hacking the US military drones that could interfere with a mission. It is a 26 dollar software.
A: I have no idea. (Note- I will leave this out)

They show me the drone.
This is the phantom 4 DJI is the company this is the one we just got; there are different models and prices. This whole set up cost about 1200 dollars - not that expensive – operated gimble system as you fly you move the camera up and down it will do stills and video and it communicates to the remote to the tablet the video what's sent isn't always great. There's an sd card.

Q: To become airborne – how can it take off and stay aloft?
Captain Cartledge and Officer Allard show that the propellers are detached from the craft, which is why at first it looks impossible for it to take off...
A: The computer system is incredible, (there are) top and bottom sonars - it knows its latitude and longitude and where it is; if we lose a signal it will return to where it took off. It knows its GPS position - it wouldn't give us the victim's GPS but would allow us to id that person's place and its flow in direct eyesight. We always know where it is based on the line of site - we have to keep it in our line of sight at all times.

Some of the smaller ones called the Mavic pro foldable can go 3 miles but the FAA still says you need to maintain line of sight.

Every time we fly we have 2 people -we have a pilot in command and a visual observer relaying to the pilot if there are any hazards or harm. If (there is a traffic) accident (we) can stay away but just view (it) from the outskirts. From the tree line we don't have to be right on top -we are standing still from the line of sight. It is pretty strictly regulated.

Q: Are you experimenting with any other technology tools?
A: In general we are a pretty progressive department. We have a lot of other things other agencies have done. We have in-housie AFIS fingerprint systems; we have a ton of things -we have criminal investigation tools others don't have. Our website is informative, but we don't put out everything about our tools (such as the most up to date ones used at a crime scene. (We have) UTD LIDAR (light detection and ranging) – (it is) light detection (in lieu of radar?) We're always looking ahead at tech and it is expensive to (keep up).

Q: Exploring preparations for acquiring drones.
We did it the right way (the preparation for drones). We're an accredited agency - we have policies for everything -we crafted drone policy before we went forward and before we even bought the drone. We try to do things the right way.

J offers to give transcript and asks about the transcript being on the web
Obtains spelling: Allard.

What's the time frame on the paper- I'd like to read it just for my own, send it before

> you (submit it to your teacher).
>
> Do you want to not have your names in there?
> You are the pilot I don't care. When you write this make it clear that all we are doing are under the jurisdiction of the FAA, get it to us before deadline and we can change it I don't want to jeopardize license.

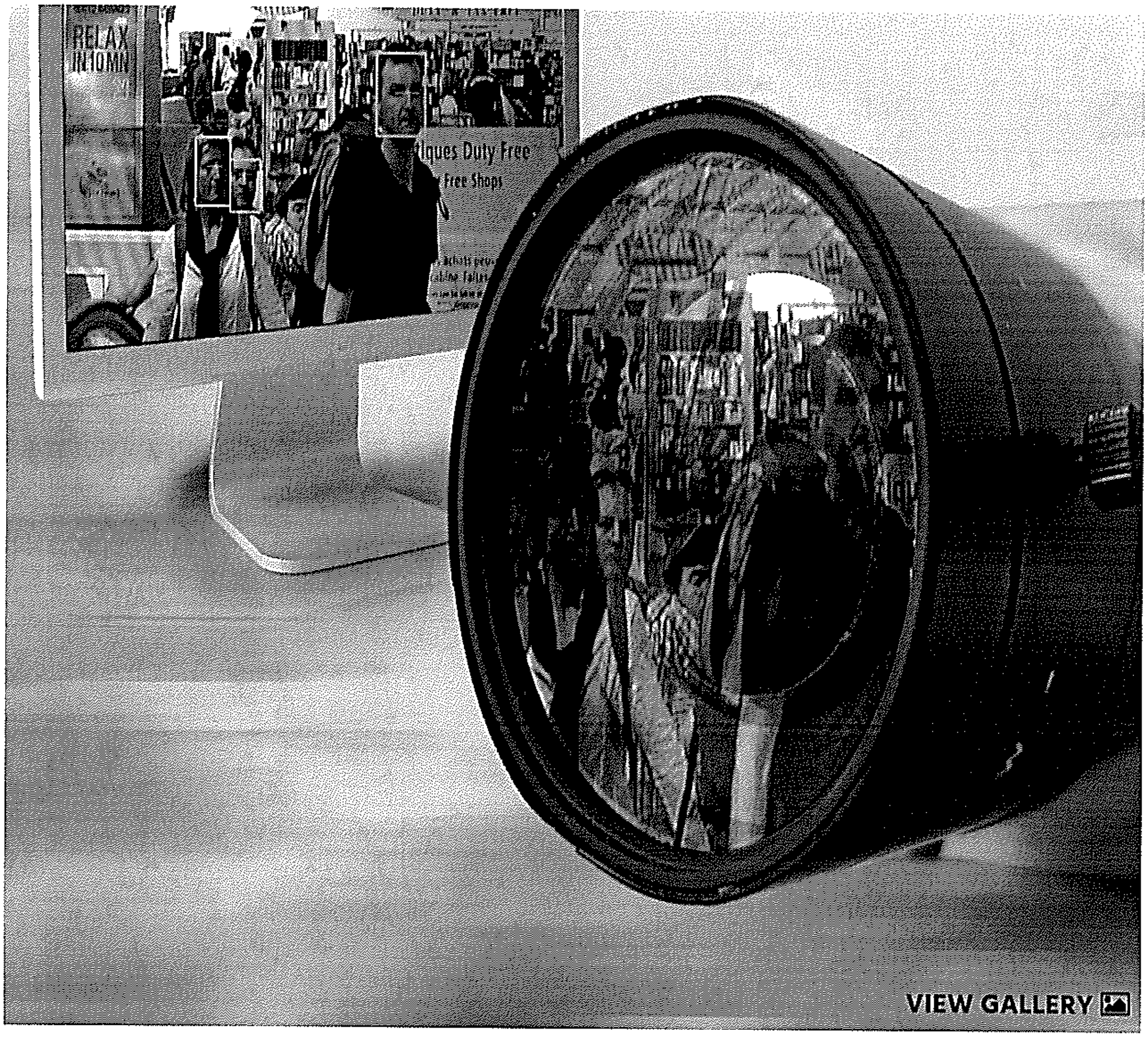
--
Respectfully.

Michael J. Allard #106
Highway Safety Officer
Crime Scene Services
AFIS Administrator

Home // Investigations // Forensics // Facial Recognition // SentiVeillance 6.0 Facial Identification and Object Recognition Technology

SentiVeillance 6.0 Facial Identification and Object Recognition Technology

NEUROTECHNOLOGY — APRIL 3, 2017



Neurotechnology released the SentiVeillance 6.0 software development kit (SDK), which provides improved facial recognition using up to 10 surveillance, security and public safety cameras on a single computer. The new version uses deep neural-network-based facial detection and recognition algorithms to improve accuracy, and it utilizes a Graphing Processing Unit (GPU) for enhanced speed. Also, now users can more quickly and easily adjust the tradeoff between speed and accuracy as needed for different applications.

"We developed SentiVeillance 6.0 as a self-adapting system based on deep neural networks that were trained on a larger quantity of data," said Ignas Namajunas, surveillance technologies research lead for Neurotechnology. "This ensures better generalization for a variety of conditions. Additionally, by making use of the GPU processing capabilities, we were able to improve the processing speed significantly."

Because SentiVeillance 6.0 can process information from up to 10 surveillance cameras with one GPU, it provides faster, easier, more accurate identification of faces against watch lists, making it suitable for a wide range of surveillance applications.

As with previous versions, the new SentiVeillance also provides real-time moving object detection; tracking and classification for pedestrians, vehicles and other predefined object classes based on size and speed of movement; and area control that triggers "events" when people or objects enter, leave or stay in restricted areas.

The SentiVeillance 6.0 SDK is available through Neurotechnology or from distributors worldwide. For more information and trial version, go to: www.neurotechnology.com. As with all Neurotechnology products, the latest version is available as a free upgrade to existing SentiVeillance customers.

REQUEST MORE INFORMATION

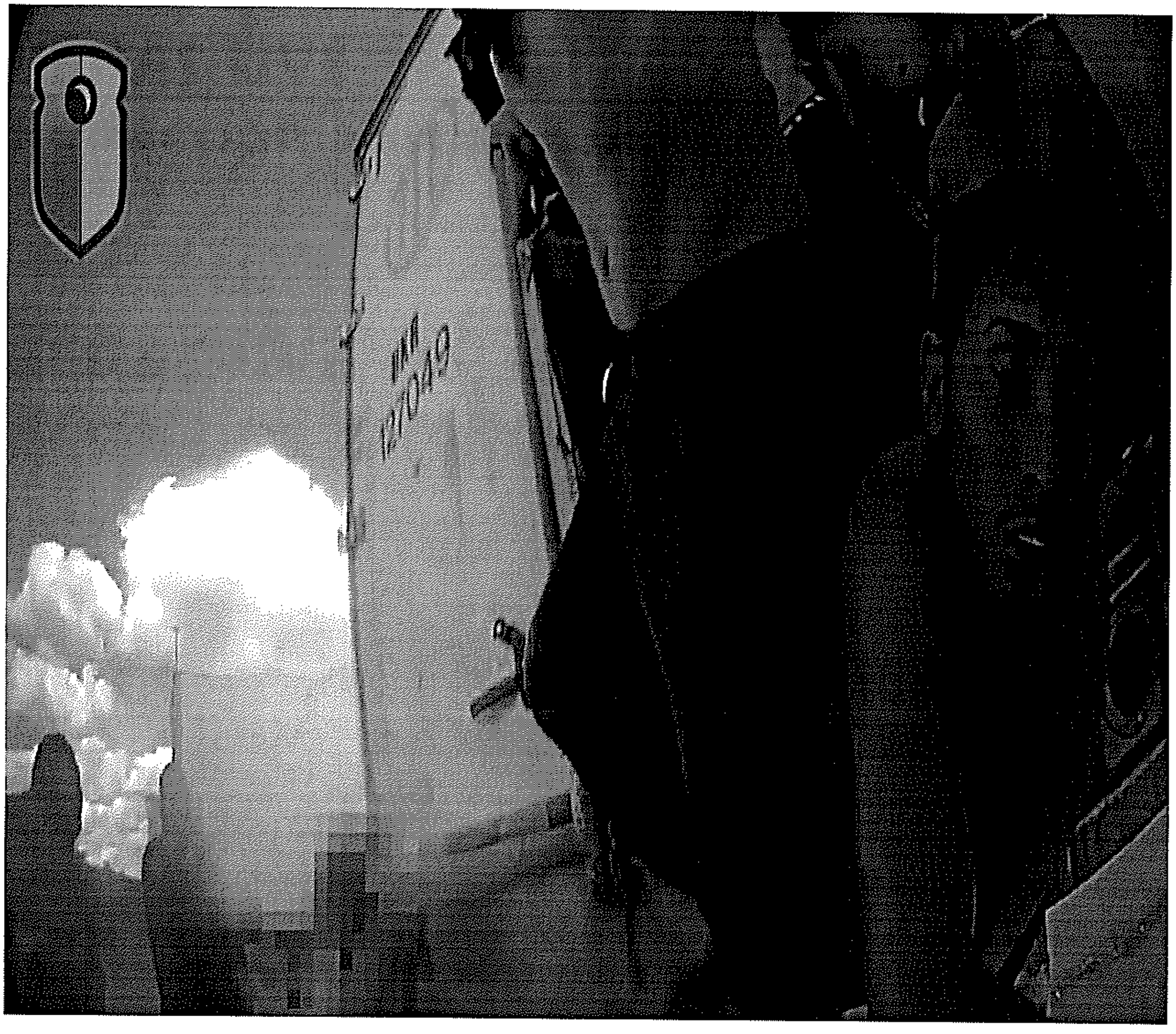
FACIAL RECOGNITION

SentiVeillance Server

Home // Investigations // Forensics // Facial Recognition // REDACTIVE - Facial Recognition-Based Redaction Software

REDACTIVE - Facial Recognition-Based Redaction Software

WATCHGUARD VIDEO — OCTOBER 19, 2016



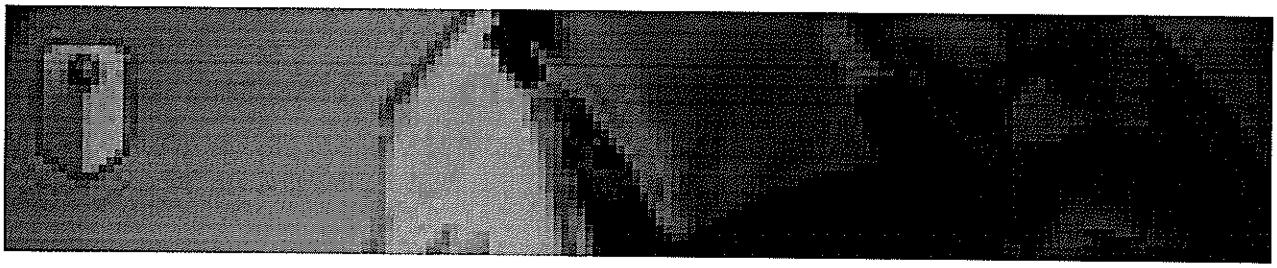
REDACTIVE is a video and audio redaction software that expedites the redaction process and eases the learning curve for evidence technicians and law enforcement officers.

REDACTIVE's advanced facial recognition technology automatically detects and identifies human faces, minimizing the elements of the video which are falsely detected as human, thus reducing the overall time spent manually searching and marking the video for redaction. Users begin the redaction process by instructing the software to auto-detect any face in the video. Once auto-detection is complete, the software allows the user to select and redact the face or faces throughout the video.

"The software is simple to use and extraordinarily powerful in its ability to accurately identify human faces quickly through an entire video clip," said Steve Coffman, President of WatchGuard.
In the wake of the FOIA Improvement Act of 2016 and ever-changing state legislation regarding treatment of video evidence, agencies are shouldering the burden of a significant increase in the quantity and complexity of redaction requests. Redaction requirements can vary from the very specific (i.e. redaction of minors) to the very broad (i.e. redaction of uninvolved bystanders). The increase is leaving agencies struggling to react accordingly.

"Today's redaction tools simply aren't keeping up, forcing agencies to either miss submission deadlines or compromise their output by delivering video that blurs out the entire screen and everything useful," added Coffman. "REDACTIVE's technology reduces the complexity, allowing the evidence technician or officer to deliver the very best redacted video evidence in the shortest amount of time possible."

REQUEST MORE INFORMATION



FACIAL RECOGNITION

Undocumented Worker Rescue Redacted Face of Minor

OFFICER.com

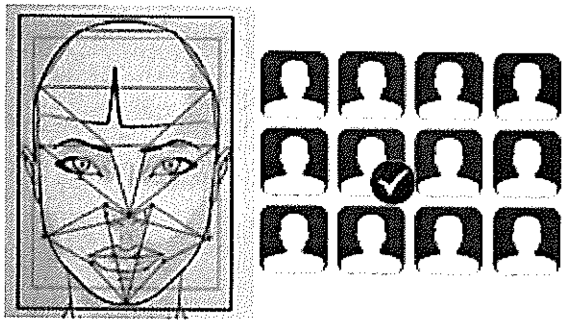
PSE & NSA Special Product Showcase

RELM WIRELESS

KNG Series | P25 Digital Radios

Meet the KNG Series digital portable radio. The one radio that works as long and as hard as you do in the same mission critical situations as you do. Compliant with APCO Project 25 specifications, the KNG Series assures uninterrupted interoperability across frequencies, different groups of responders and variation in terrain. Bk Radios are proven tough and reliable with a long battery life.

www.relm.com



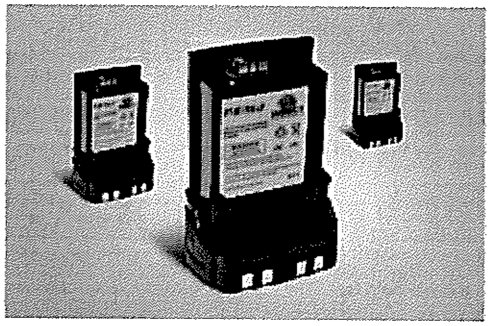
VIGILANT SOLUTIONS

NSA Booth #1102

Think you can't use facial recognition? Think again.

Stumped by less than perfect probe images? Don't throw away images with poor lighting, bad angles, or closed eyes. Our easy-to-use facial recognition turns less than perfect images - including those from ATMs, security cameras or social media - into new leads to help solve cases faster. Agencies of all sizes benefit from facial recognition & now Vigilant puts that technology within reach for all.

Download our whitepaper: Facial Recognition Art or Science?



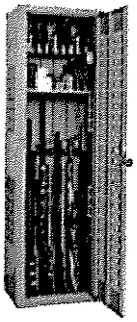
AWARD-WINNING BATTERY POWERS MOTOROLA APX RADIOS

IPT-MT7038-LiP replacement battery for Motorola APX 6000/7000/8000 radios wins Communications Solutions Product of the Year! Impact Power Technologies LifeSaver Series™ use proprietary Lithium Polymer chemistry guaranteeing 20-hours runtime & 900 recharges—3-4x more than OEM—without voiding warranty. Save lives &

IMPACT
Power Technologies, LLC
Voted Best Product at IACPI

money with full shift power. NEW Performance Guarantee & Battery Buy-Back Recycling!

Save at impactpowertech.com/LETR



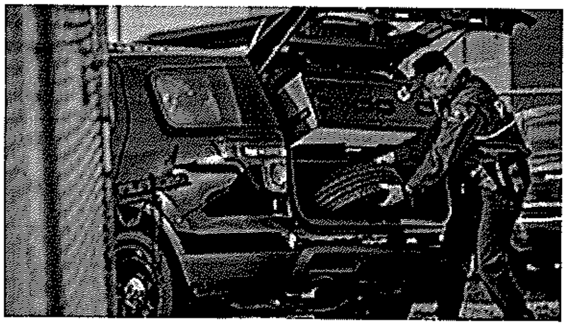
Lock, Load and Win with ArgosSECURITY™ by Datum®!

Argos Security™ by Datum® is a unique line of weapon storage cabinets, armorer's benches and rack systems to outfit any armory, evidence storage area or weapons facility. Contact us today to learn how Argos can equip your armory with the latest in versatile, secure, fully customizable weapons storage. Now with eighteen National Stock Numbers. (NSN) Made in USA.

Argos SECURITY
by DATUM

www.argosweaponstorage.com

PSE Booth #1722

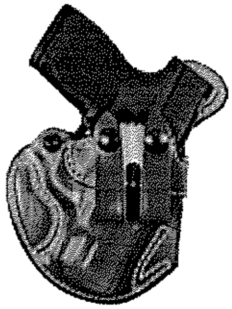


TruckVault "Lift Technology"

TruckVault prides itself in manufacturing a secure in-vehicle storage solution for virtually every vehicle on the road. One of the most popular Public Safety vehicles is the Ford Explorer PPV and integral in the rear crash safety of this vehicle is its in-vehicle spare tire. Our TruckVault "Lift Technology" spare access system combines form with function using air assist cylinder.

TRUCK VAULT

www.truckvault.com



NEW DESANTIS PRODUCT AVAILABILITY FOR S&W M&P SHIELD .45

The Cozy Partner®, Style 028 is 1 out of 17 new holster fits for the S&W Shield .45 This holster features a tension device and precise molding for handgun retention. A memory band retains the holster's shape for easy one handed re-holstering. 1 3/4" split belt loop is standard. DeSantis didn't invent concealment, they just perfected it!

Officer.com / Contact Us / Advertise

If you are having trouble viewing, please **click here**.

This e-mail is being sent to **mallard@northamptonma.gov**.

Please add mail.officer.com to your address book or safe sender list to receive our emails in your inbox.

Unsubscribe | Manage Newsletter Subscriptions | Change E-mail | Forward to a Friend | Customer Service Center | Privacy Policy

If this e-mail was forwarded to you and you are interested in subscribing to our emails, please **click here** to sign-up.

If you have trouble with any of these methods, you can reach us toll-free at 800-547-7377.

Officer.com
SouthComm Business Media, LLC
1233 Janesville Ave
Fort Atkinson, WI 53538

News (/news) Photos (/photo-galleries) Blogs (/blogs) Videos (/videos) Cop Slang (/cop-slang)

How-To's (/whitepapers) Magazine (/issues) Products (/products) Jobs (http://policecareerfinder.com/)

Directory (http://directory.policemag.com/) Webinars (/webinars)

Newsletters (https://bob.dragonforms.com/init.do?omedasite=BOB6226_PZpref)

POLICE THE LAW ENFORCEMENT MAGAZINE (/) COMMUNITY FOR COPS

Search SEARCH

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle Ops (/vehicle-op

TECHNOLOGY

Amazon Employees Join ACLU, Investors in Protest of Amazon's Sale of Tech to Police

June 22, 2018 • by Staff Writer (/authors/504428/staff)

Embed from Getty Images (http://www.gettyimages.com/detail/952605500)

In a letter posted to an internal company Wiki page and later obtained by The Hill (http://thehill.com/business-a-lobbying/393583-amazon-employees-protest-sale-of-facial-recognition-tech-to-law), a group of Amazon employees have asked company executives to discontinue its sale of the company's Rekognition facial recognition software to law enforcement agencies. They also asked the company to stop providing services to a company called Palantir — a data analytics concern that provides "mission critical software" to Immigration and Customs Enforcement (ICE) in support of their detention and deportation efforts.

"We refuse to build the platform that powers ICE, and we refuse to contribute to tools that violate human rights. As ethically concerned Amazonians, we demand a choice in what we build, and a say in how it is used," the document said.

The letter, addressed directly to Amazon CEO Jeff Besos, said. "Along with much of the world we watched in horror recently as U.S. authorities tore children away from their parents ... we are deeply concerned that Amazon is implicated, providing infrastructure and services that enable ICE and DHS."

The employees' action follows closely on the heels of another effort by the ACLU and a group of company investors (https://www.policemag.com/blog/technology/story/2018/06/balancing-privacy-rights-and-facial-recognition-technology-for-police.aspx).

Read more about technology (/tags?tag=technology) Facial Recognition (/tags?tag=Facial+Recognition) Amazon Web Services (/tags?tag=Amazon+Web+Services)

0 Comments

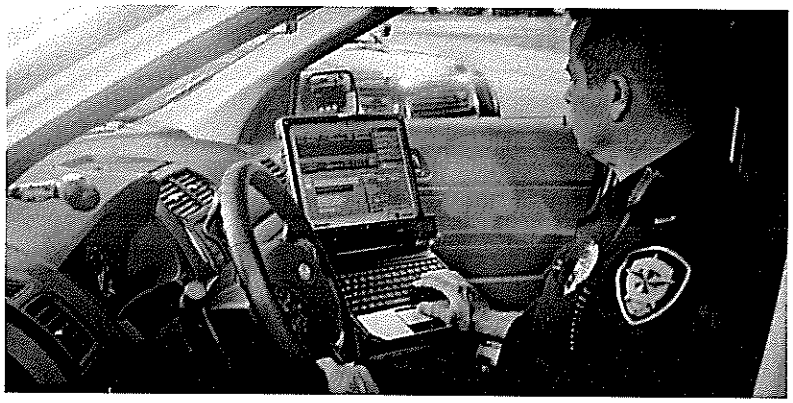
Join the discussion...

MORE

TECHNOLOGY

NEWS (/NEWS)

Panasonic to Take Part in Panel at IACP Technology Conference (/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)



(/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)
The IACP Technology Conference is taking place in Jacksonville, FL, May 20–22. At the event on Tuesday, May 21, at 4 pm ET, Panasonic will take part in the panel discussion, "Managing Officer Safety Now and in the Future through a Strong Technology Ecosystem."

OFFICER FAVORITES (/ISSUES)

- Tactical Gear (https://www.policemag.com/tag tag=Tactical+Gear)
- How-to Guides (https://www.policemag.com/tag tag=How-To+Guides)
- Officer Fitness (https://www.policemag.com/tag tag=Officer+Fitness)
- Drug Cartels (https://www.policemag.com/tag tag=drug+cartels)

NEWS (/NEWS)

Video: Could a Robot Make Traffic Stops Safer? (/512502/video-could-a-robot-make-traffic-stops-safer)

(/512502/video-could-a-robot-make-traffic-stops-safer)

Once the officer's vehicle is parked behind the motorist's car, GoBetween rolls up to the driver's side window of the motorist, where it becomes the officer's eyes, ears and mouth. A spike strip automatically placed in front of the car's rear wheels keeps the motorist from driving away until the traffic stop is completed.

NEWS (/NEWS)

Knightscope Adds Facial Recognition to K1 Security Robots (/512416/knightscope-adds-facial-recognition-to-k1-security-robots)

"Prospective clients were able to upload a photo into the Knightscope Security Operations Center (KSOC) and then watch the K1 detect and report them as they moved about the booth. One creative individual even attempted to elude 'capture' by donning a pair of dark sunglasses to no avail," the company says.

NEWS (/NEWS)

Gamber-Johnson Wins WI Governor's Export Achievement Award (/512377/gamber-johnson-wins-wi-governors-export-achievement-award)

Gamber-Johnson has been named the recipient of the 2019 Governor's Export Achievement Award by the Wisconsin Economic Development Corporation (WEDC) for its contribution to Wisconsin's exporting strength.

- Stupid Criminals (https://www.policemag.com/tag tag=Stupid+Criminals)
- Shots Fired (https://www.policemag.com/tag tag=Shots+Fired)
- Police Humor (https://www.policemag.com/tag tag=Police+Humor)
- Defensive Tactics (https://www.policemag.com/tag tag=Defensive+Tactics)

COP SLANG (HTTPS://POLICEMAG.COM/COP-SLANG)

Top Terms (https://policema slang) (https://policemag.cc slang)

Badge Bunny
(https://www.policemag.com/cop-
slang/badge-
bunny)
Blue Falcon
(https://policemag.com/cop-
slang/blue-
falcon)
Lot Lizard
(https://policemag.com/cop-
slang/lot-lizard)

Zebra
(https://www.
slang/zebra)
Personal
(https://polic
slang/persor
Vox
(https://polic
slang/vox)

VIEW TERMS (HTTPS://POLICEMAG.C

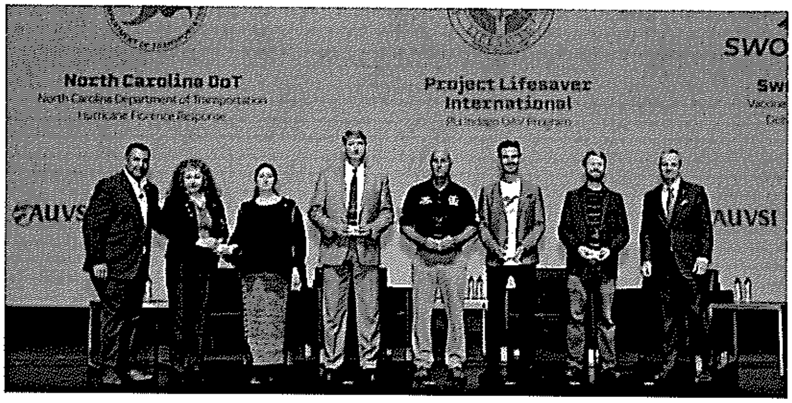
NEWS (/NEWS)

San Francisco Could Ban Use of Facial Recognition by Law Enforcement (/512178/san-francisco-could-ban-use-of-facial-recognition-by-law-enforcement)

The proposal, introduced by San Francisco Supervisor Aaron Peskin, would also require public input and the supervisors' approval before agencies buy investigative technology with public funds. That includes the purchase of license plate readers, toll readers, closed-circuit cameras, body cams, and biometrics technology and software for forecasting criminal activity.

NEWS (/NEWS)

Project Lifesaver International Receives Prestigious International Humanitarian Award (/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)


North Carolina DoT
North Carolina Department of Transportation
Hurricane Florence Response
Project Lifesaver International
SWO
AUVSI
AUVSI

(/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)
Project Lifesaver International (PLI) has been awarded the Humanitarian Xcellence Award by the Association for Unmanned Vehicles Systems International for its use of DJI drones to locate missing persons.

NEWS (/NEWS)

Transcend Tactical Introduces Mobile Gas Deployment System for Robots (/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

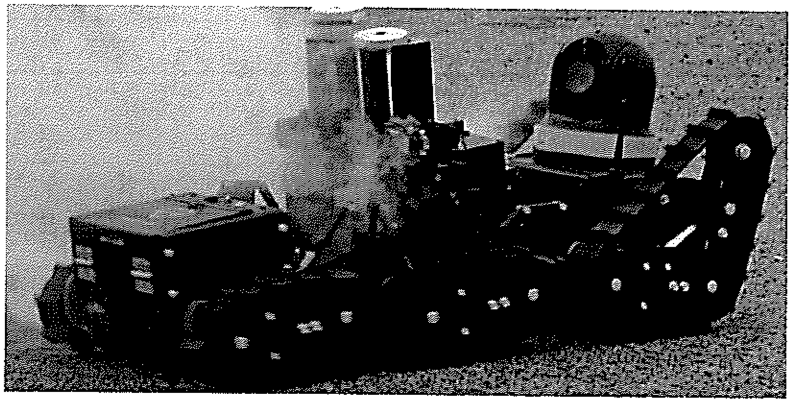
✉ Newsletter

Email Address SUBMIT

MAGAZINE (/ISSUES)

January 2019

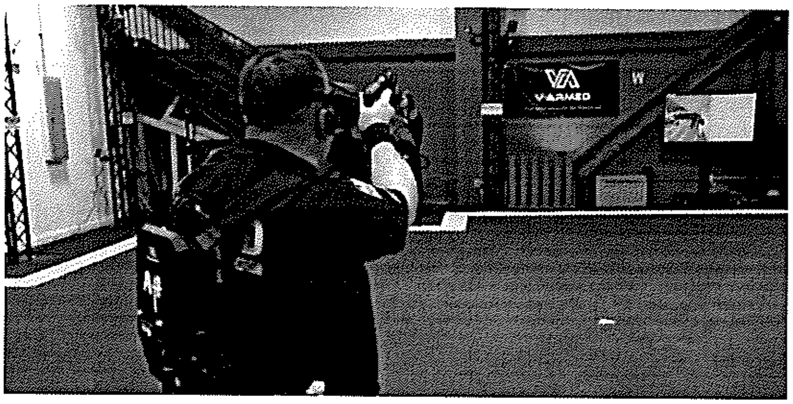
Digital Edition (/digitalmagazine)
Digital Archives (/digitalarchives)
Subscribe (/subscribe)



(/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)
Transcend Tactical has launched a gas deployment system that can be added to its Vantage robot to deploy two hot or cold gas grenades remotely and with mobility.

NEWS (/NEWS)

NYPD Testing Virtual Reality-Based Training (/511543/nypd-testing-virtual-reality-based-training)



(/511543/nypd-testing-virtual-reality-based-training)
The NYPD is testing a virtual reality scenario-based training system. About 200 officers participated in the training program, which was conducted earlier this month at a state-of-the-art facility in Williamsburg, Brooklyn.

NEWS (/NEWS)

Axon Develops Tool for Measuring Officer Performance and Identifying Training Needs Through Body Camera Footage (/511538/axon-develops-tool-for-measuring-officer-performance-and-identifying-training-ne)

Axon has announced the launch of Axon Performance, a data analytics tool that helps to streamline the policy review process for law enforcement agencies. Axon Performance allows supervisors to more efficiently review video footage, perform agencywide officer performance evaluations, identify training needs and save officers time so they can spend more time in their communities.

LOAD MORE (/362462/AMAZON-EMPLOYEES-JOIN-ACLU-INVESTORS-IN-PROTEST-OF-AI

✉ Don't Miss Another Story

Email Address SUBMIT

Topics

Training & Careers (/training-careers)
Special Units (/special-units)
Patrol (/patrol)
Technology (/technology)
Vehicle Ops (/vehicle-ops)
Weapons (/weapons)
Point of Law (/point-of-law)
Procedures & Policies (/procedures-policies)
Investigations (/investigations)
Command (/command)

Essentials

News (/news)
Photos (/photo-galleries)
Videos (/videos)
Blogs (/blogs)
How-To's (/whitepapers)
Magazine (/issues)
Products (/products)
Jobs (http://policecareerfinder.com/)

Services

Subscription (/subscribe)
Advertise (/advertise)
Contact Us (/contact-us)
Online Store (http://store.policemag.com/)
Privacy Policy (https://www.bobitbusinessmedia.com/privacy-policy/)
Newsletter Sign Up (https://bob.dragonforms.com/init.do?omedasite=BOB6226_PZpref)

Connect

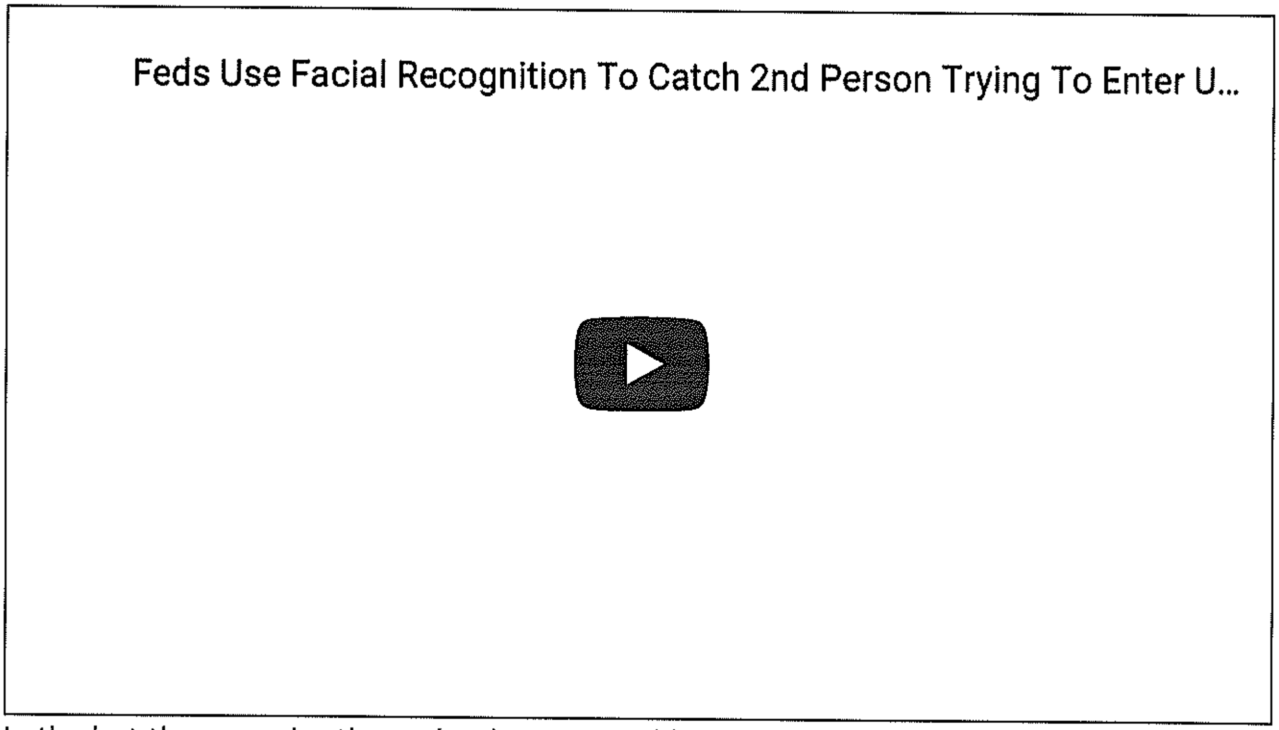
Suppliers Directory (http://directory.policemag.com/?ref=ftr)

Home // Investigations // Forensics // Facial Recognition // Feds Use Facial Recognition to Catch 2nd Person Trying to Enter U.S. Illegally

Feds Use Facial Recognition to Catch 2nd Person Trying to Enter U.S. Illegally

In the last three weeks, the technology at Washington's Dulles International Airport has been used to catch two imposters trying to illegally enter the U.S.

SEP. 12, 2018



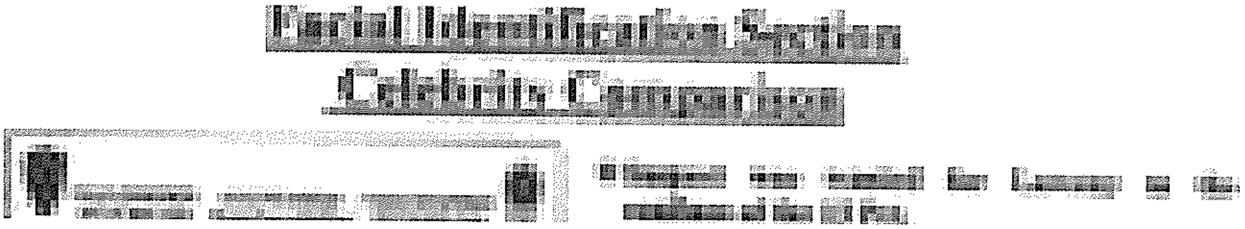
Feds Use Facial Recognition To Catch 2nd Person Trying To Enter U...

In the last three weeks, the technology at Washington's Dulles International Airport has been used to catch two imposters trying to illegally enter the U.S.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?



FACIAL RECOGNITION

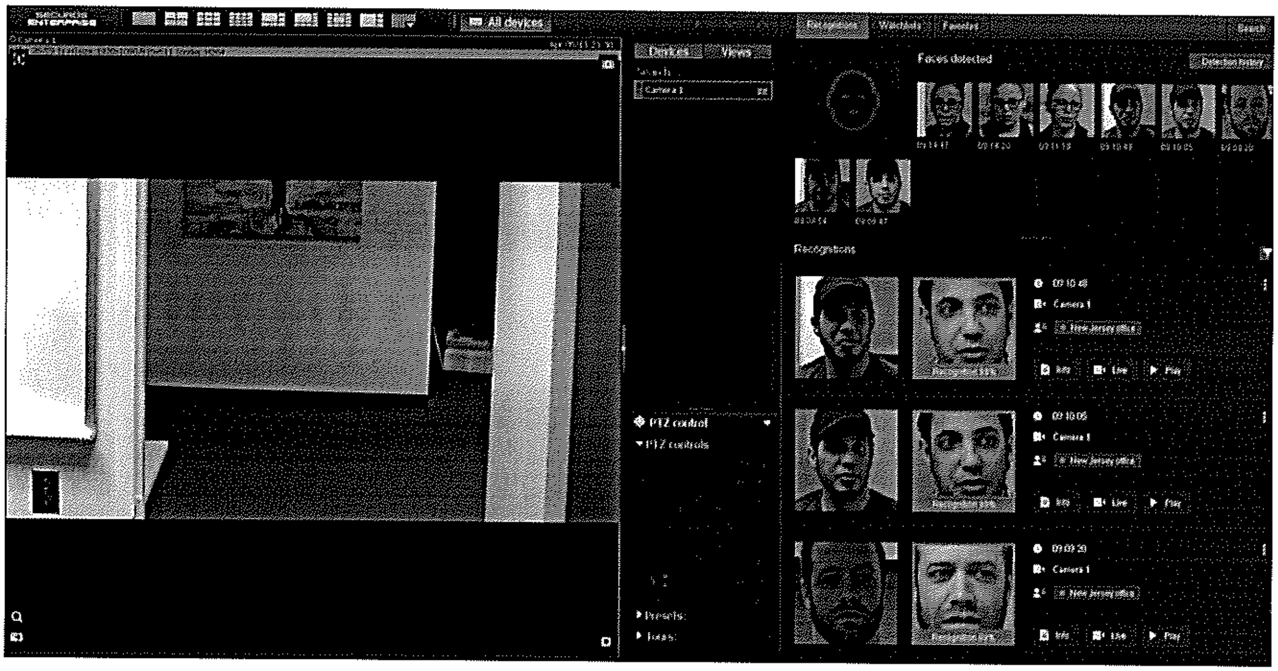
Report: NYPD Using Celebrity Photos to Track Down Criminals

Home // Investigations // Forensics // Facial Recognition // At ISC West 2019: New SecurOS FaceX Analytics from ISS Sets New Benchmarks

At ISC West 2019: New SecurOS FaceX Analytics from ISS Sets New Benchmarks

New SecurOS™ FaceX Analytics from ISS Sets New Benchmarks in Facial Recognition

INTELLIGENT SECURITY SYSTEMS (ISS) — APRIL 10, 2019



INTELLIGENT SECURITY SYSTEMS

Las Vegas, NV (April 10, 2019) – ISS – Intelligent Security Systems, a leading provider of intelligent VMS and native analytics globally, is demonstrating the company's new powerful SecurOS™ FaceX facial recognition solution here at ISC West 2019 (booth #28073). FaceX delivers the unique capability to accurately recognize individuals' faces from different camera angles with a host of specific facial characteristics under various lighting conditions. The new native analytics solution is built on the basis of ISS' recently enhanced SecurOS v.10 Video Management System (VMS) platform, embedding all of FaceX's functionality including the ability to add and import files, perform searches and more.

"Our new SecurOS™ FaceX Facial Recognition Solution provides a significant leap in performance and capabilities for a wide range of surveillance and business intelligence applications. Its enhanced ability to accurately capture and identify individuals using profile images and facial characteristics greatly expands the range of applications for facial recognition across numerous surveillance and business intelligence applications," said Shawn Mather, Director of Sales for U.S., ISS. And unlike conventional facial recognition analytics, FaceX is fully built specifically to perform with the SecurOS™ VMS platform, enabling seamless control of all analytics functions and management directly through the VMS."

SecurOS™ FaceX sets a new benchmark in facial recognition analytics by dramatically expanding the ability to identify and match faces with greater versatility. Most notable is that FaceX resolves longstanding challenges for facial recognition related to camera viewing angles, facial expressions and diverse lighting conditions, providing for a far greater range of identity matches and authentication. FaceX compares captured images against databases of known individuals, or faces captured from video streams, expanding the use of facial recognition to search for individuals during unfolding events. Searches can also be conducted by specific facial features against multiple watchlists and a virtually unlimited database of facial images. FaceX also supports multi-factor authentication for implementation with access control systems.

SecurOS™ FaceX also incorporates Advanced Neural Network (ANN) technologies enabling a whole new host of features and capabilities. In addition to expanding facial detection to include profile images, FaceX can clarify a database search based on specific face features such as age, gender and ethnicity, as well as by hair color, the presence of facial hair, glasses, headwear and bald patches.

Additional features include: searches by photo or screenshot; consecutive face searches; integration with multiple watchlists; unlimited face recognition database size; multiple watchlists and database management capabilities; batch import of images into face recognition databases; auto detection of redundant facial images; centrally managed distributed, scalable architecture; and image-based monitoring of captured faces and recognized faces. SecurOS™ FaceX also provides detailed reporting and metrics to aggregate data for forensic investigations.

SecurOS™ FaceX Facial Recognition Solution will be available in April, 2019.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

Posted Bytcsmmoat Apr 21 2019 19:54

I would like to use this but not pay for it... Hmmm... Oh well, looks like im gonna get re-embersed!

FACIAL RECOGNITION

SecurOS FaceX Analytics

Home // Investigations // Forensics // Facial Recognition // Safr Facial Recognition Solution

Safr Facial Recognition Solution

MOC1 SOLUTIONS, A DIVISION OF MOBILE OFFICE COMMUNICATIONS INC. — MARCH 21, 2019

- Add facial recognition to employee badge access for faster, more secure entry
- Screen restricted areas via CCTV integration to ensure everyone there should have access
- Provide alerts for unknown individuals, preventing "tailgating" through restricted doors
- Integrate with staff databases to quickly onboard your entire crew

The Safr platform is built with the following core design principles:

- World class accuracy
- Designed specifically to recognize faces in real-world conditions, including people in motion, in dim lighting, at occluded angles and with heavy make-up
- Scalable: can reliably match against millions of faces in under a second
- Affordable. A modern architecture that leverages edge computing and avoids sending massive amounts of data to the cloud for recognition

Example Use Cases:

- Reduce entry friction with "Face Ticket"
- ID VIPs for special greeting or premium
- "Face Pay" at concession or merchandise stands
- Locate lost loved ones
- Deliver VIP messages
- Earn loyalty rewards as you traverse the venue
- Kiosks can be installed to try to give better service to the customers and send orders directly to maintain efficiency.

For the standalone product, a low monthly per-camera fee is charged. The fee is determined by the number of cameras using the facial recognition capability, the implementation platform and the cloud platform being used (on-premise or Safr remote cloud). The Safr system can be deployed on-premise using the clients existing cloud infrastructure or, by using the remote Safr cloud infrastructure.

MOC1 Solutions offer Safr as a turnkey cloud based on-premise solution to meet the client's needs. AstraTAC and Safr are now available on the US Government's GSA Schedule at: www.gsaadvantage.gov.

REQUEST MORE INFORMATION

FACIAL RECOGNITION

SecurOS FaceX Analytics

New Facial Recognition Solution Available

MOC1 SOLUTIONS, A DIVISION OF MOBILE OFFICE COMMUNICATIONS INC. — MARCH 14, 2019

March 14, 2019, Washington DC, RealNetworks, a Seattle Washington based company, inventor of streaming video and now the leader in Facial Recognition and MOC1 Solutions a division of Mobile Office Communications Inc. have formed a strategic partnership to offer Safr Facial Recognition solution to the public and private sectors. MOC1 Solutions intend to market the solution as either a standalone product or, integrated with their AstraTAC solution to provide companies with an affordable command and control capability along with integrated real-time facial recognition using virtually any existing digital IP camera. The facial recognition capability sold as a stand-a-lone solution provides companies with an extra level of security as well as provide for payment processing which can reduce identity and financial theft, increase transaction processing speed, and increase convenience for consumers by eliminating the need for physical and mobile wallets.

The Safr platform is built with the following core design principles:

- World class accuracy
- Designed specifically to recognize faces in real-world conditions, including people in motion, in dim lighting, at occluded angles and with heavy make-up
- Scalable: can reliably match against millions of faces in under a second
- Affordable. A modern architecture that leverages edge computing and avoids sending massive amounts of data to the cloud for recognition

Example Use Cases:

- Reduce entry friction with "Face Ticket"
- ID VIPs for special greeting or premium

- "Face Pay" at concession or merchandise stands
- Locate lost loved ones
- Deliver VIP messages
- Earn loyalty rewards as you traverse the venue
- Kiosks can be installed to try to give better service to the customers and send orders directly to maintain efficiency.

Vendor Security:

- Add facial recognition to employee badge access for faster, more secure entry
- Screen restricted areas via CCTV integration to ensure everyone there should have access
- Provide alerts for unknown individuals, preventing "tailgating" through restricted doors
- Integrate with staff databases to quickly onboard your entire crew

For the standalone product, a low monthly per-camera fee is charged. The fee is determined by the number of cameras using the facial recognition capability, the implementation platform and the cloud platform being used (on-premise or Safr remote cloud). The Safr system can be deployed on-premise using the clients existing cloud infrastructure or, by using the remote Safr cloud infrastructure.

MOC1 Solutions offer Safr as a turnkey cloud based on-premise solution to meet the client's needs. AstraTAC and Safr are now available on the US Government's GSA Schedule at: www.gsaadvantage.gov. Quantity discounts are available.

For more information on Safr Facial Recognition and AstraTAC
visit www.moc1solutions.net.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?

FACIAL RECOGNITION

SecurOS FaceX Analytics

Home // Investigations // Forensics // Facial Recognition // FacePRO® Facial Recognition Server Software

FacePRO® Facial Recognition Server Software

PANASONIC SYSTEM COMMUNICATIONS CO. OF NORTH AMERICA — APRIL 9, 2018

Panasonic System Solutions Company of North America, Security Group, introduces FacePRO®, a deep learning facial recognition system using extreme sensing and enhanced detection technology to identify persons of interest and alert authorities of their presence in real-time. FacePRO high-precision facial recognition software can identify faces that are difficult to recognize with conventional technologies, including faces at an angle of up to 45 degrees to the left or right or 30 degrees up or down, even those partially hidden by sunglasses.

The new software, which fits into the Panasonic unified and secure ecosystem, features the "iA (intelligent Auto) mode" that automatically adjusts settings for the camera to shoot optimal images best suited for facial recognition. When used with Panasonic's i-PRO EXTREME series network cameras installed with the included "Best Shot License Key", only the "Best Shots" will be sent to the server for facial recognition. The combination of Panasonic core devices and the facial recognition software maximizes performance to achieve high-precision recognition. The company plans to add a function to recognize partially covered faces with a surgical mask, which is difficult with conventional systems, by the end of this year.

Additionally, using FacePRO software with cameras equipped with the iA function enables image analysis to be performed on the camera instead of the server to send only the best images to the server. This will result in reducing server and network loads, which leads to overall system cost reductions. When 10 or more network cameras are connected to the system, the cost can be reduced by up to 50% compared to conventional systems that do not use the Best Shot function.

ℹ **REQUEST MORE INFORMATION**

FACIAL RECOGNITION

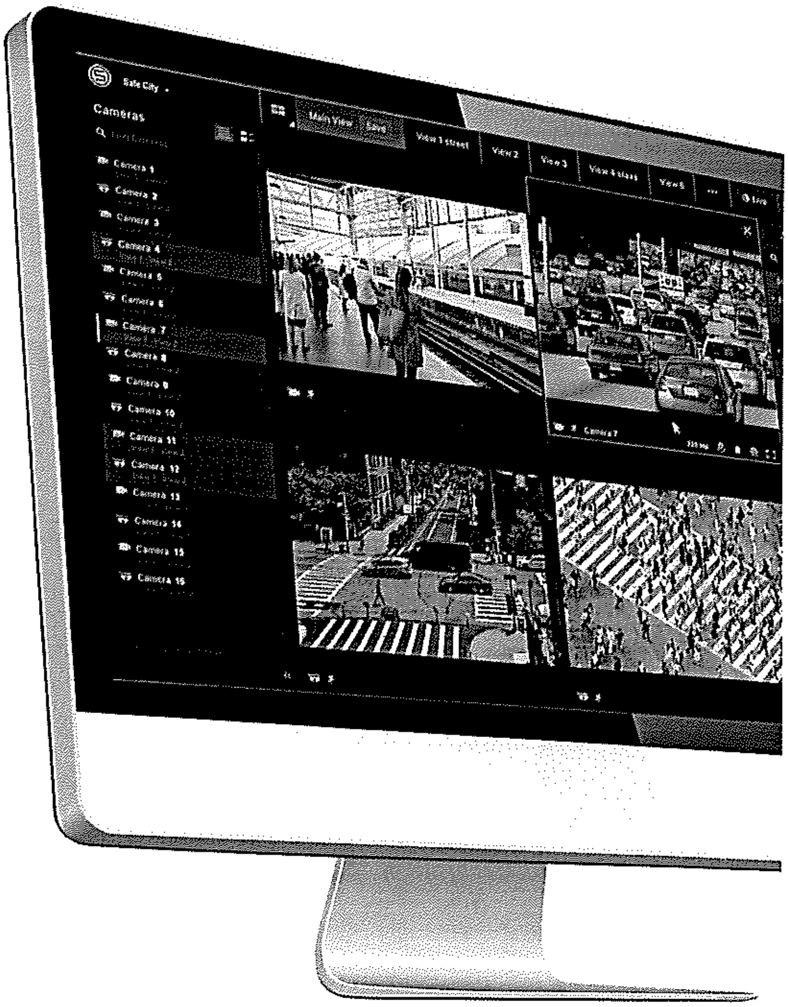
SecurOS FaceX Analytics

Home // Command/HQ // Technology // Traffic // Traffic Surveillance // At ISC West 2019: ISS Debuts New Analytics & Enhanced VMS

At ISC West 2019: ISS Debuts New Analytics & Enhanced VMS

Introductions Include New Facial Recognition and Crossroad Traffic Violation Detection Solutions

INTELLIGENT SECURITY SYSTEMS (ISS) — APRIL 10, 2019



INTELLIGENT SECURITY SYSTEMS

Las Vegas, NV (April 10, 2019) – ISS – Intelligent Security Systems, a leading provider of intelligent VMS and native analytics globally, is demonstrating the latest additions to the company's portfolio of advanced analytics developed to compliment the company's recently enhanced SecurOS™ v.10 Video Management System (VMS) here at ISC West 2019 (booth 28073). Showcased is ISS' new SecurOS™ FaceX Facial Recognition Solution that significantly expands the ability to accurately recognize faces from different camera angles along with facial expressions under various lighting conditions. Also featured is the company's new SecurOS™ Crossroad Traffic Violation Detection Solution that provides real-time detection of complex traffic violations. Both new analytics solutions complement VMS and hardware solutions from ISS that are designed to integrate with municipalities command and control systems, and capitalize on ISS' unique ability to provide metadata and video streams for advanced specialized surveillance applications.

"The introduction of ISS' new SecurOS™ FaceX Facial Recognition and SecurOS™ Crossroad Traffic Violation Detection Solutions exemplify how ISS continues to pioneer the development and deployment of new Artificial Neural Network (ANN) technologies to deliver intelligent analytics with advanced capabilities," said Shawn Mather, Director of Sales for U.S., ISS. "Whether used in conjunction with our powerful suite of SecurOS™ VMS solutions, or with third party software, ISS is continually developing new and enhanced intelligent analytics that leverage our expertise in neural networks to deliver superior performance for a wide range of applications."

SecurOS™ FaceX sets a new benchmark in facial recognition analytics by dramatically expanding the ability to identify and match faces with greater versatility. Most notable is that FaceX resolves longstanding challenges for facial recognition related to camera viewing angles, facial expressions and diverse lighting conditions, providing for a far greater range of identity matches and authentication. FaceX compares captured images against databases of known individuals, or faces captured from video streams, expanding the use of facial recognition to search for individuals during unfolding events. Searches can also be conducted by specific facial features against multiple watchlists and a virtually unlimited database of facial images. FaceX also supports multi-factor authentication for implementation with access control systems. SecurOS™ FaceX Facial Recognition Solution will be available in April, 2019.

SecurOS™ Crossroad Traffic Violation Detection Solution is powered by ISS' SecurOS™ Auto ANPR (Automatic License Plate Recognition) to provide real-time detection of complex traffic violations with highly accurate identification of the vehicle committing the infringement. SecurOS™ Crossroad monitors multiple vehicles and pedestrian behavior at intersections and potentially hazardous roadways. The turnkey solution automatically detects vehicles that run red lights and stop-signs, are travelling in the wrong direction, not following road signs or yielding to pedestrians, and various other violations. Designed to seamlessly integrate with Safe City systems, SecurOS™ Crossroad also generates detailed traffic statistics data, which can be used in municipalities' traffic management systems. SecurOS™ Crossroad Traffic Violation Detection Solution will be available in April 2019.

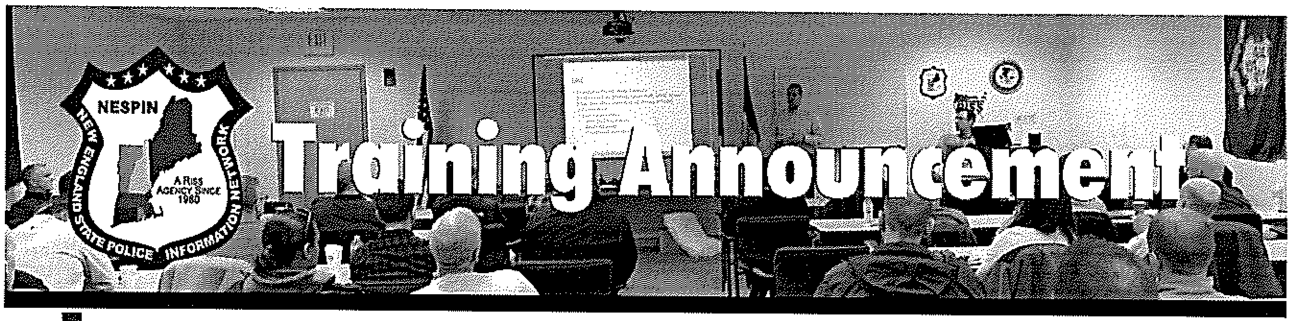
ISS is also featuring its recently enhanced **SecurOS™ v.10 VMS** (pictured above) supported by a powerful suite of native intelligent analytics, along with SecurOS™ Smart NVR, an all-in-one video management appliance. ISS' unique combination of a natively developed VMS platform and portfolio of advanced analytics ensures seamless integration of customized video management and control solutions for a wide range of surveillance and business intelligence applications.

ISS' recently formed partnership with Intel on Artificial Neural Networks provides the foundation for the development of higher levels of intuitive integrated physical security solutions employing advanced AI.

Join the conversation!

This site requires you to **login** or **register** to post a comment.

No comments have been added yet. Want to start the conversation?



ORGANIZED RETAIL CRIME TRAINING
NOVEMBER 1-2, 2018
GREENWICH PD 11 BRUCE PLACE, GREENWICH CT

ORGANIZED RETAIL CRIME TRAINING
NOVEMBER 1-2, 2018
GREENWICH PD 11 BRUCE PLACE, GREENWICH CT

Training is free for all law enforcement and retail crime investigators.Â CT POST review training credits are anticipated.

The following training is expected: Â Â Retail Crime Investigations For New Patrol Officers & Loss Prevention InvestigatorsÂ Investigating Organized Retail Crime (ORC) Rings Â Rapid Identification of counterfeit credit/debit/gift cards & the Impact On Retail Fraud in an EMV WorldÂ Indicators of Access Device Trafficking During Motor Vehicle Interdiction Stops Traditional/Gas Pump/POS and ATM Skimming & Malware in a retail EnvironmentÂ Conducting Internal Fraud InvestigationsÂ â€œThe Queen of Fraudâ€ (ID Theft/Phishing/Retail Fraud Federal Investigation Case Study Using Facial Recognition Evidence in Retail Fraud Investigations How Intelligence Sharing Can Help Solve Investigations ORC Panel Discussion (TBA)

Please go to the following link for complete details:

https://extranet.riss.net/public/53161476-9277-4552-918b-3b4359fd9655

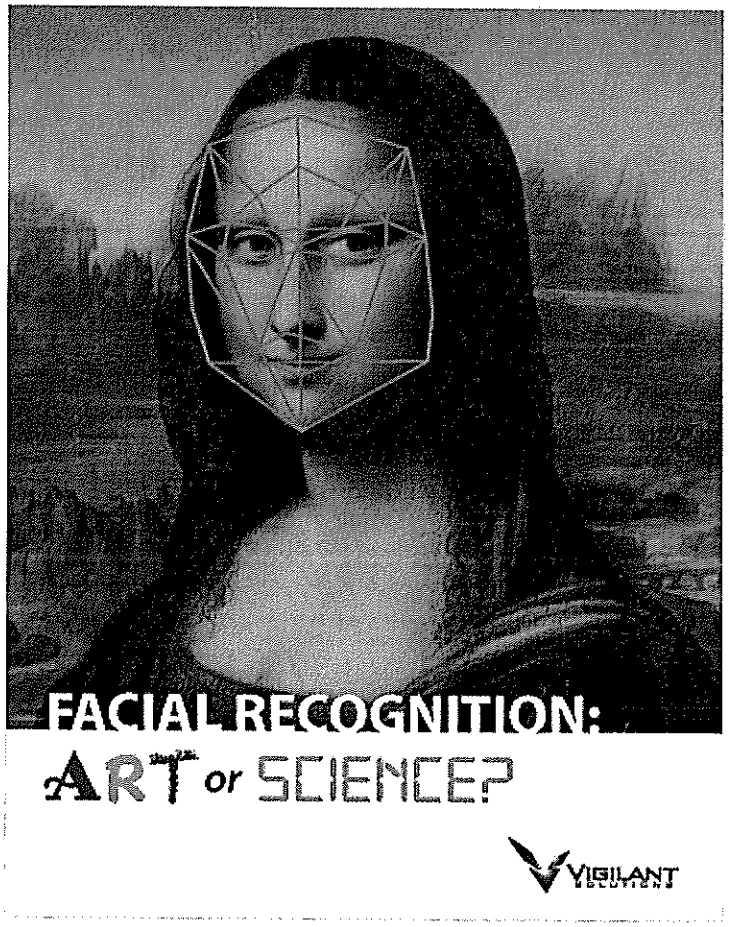
A PROVEN RESOURCE FOR LAW ENFORCEMENT
RISS
WSIN • RMIN • MOCIC • ROCIC • MAGLOCLEN • NESPIN

Share this email:

WHITEPAPERS

Host Your Whitepaper (/advertise)

Facial Recognition: Art or Science?



Generating a list of high-quality leads using facial recognition technology is now within reach for agencies of all sizes. Learn how facial recognition works, best practices for capturing probe images, and new breakthrough image pre-processing techniques that anyone can employ.

By Vigilant Solutions

Required *

First Name *

Last Name *

Job Title *

Company Name *

Email Address *

Address *

Department/Mail Stop

City *

State/Province

- Select -

Zip/Postal Code *

Country *

- Select -

Phone Number *

Type of agency *

- Select -

Your job classification *

- Select -

Size of department (sworn officers) *

- Select -

Please select your assignment *

(select all that apply)

□ Administration/Support
□ Air Enforcement
□ Armory/Firearms/Range
□ Bicycle Patrol
□ Bomb Squad/Hazardous Devices
□ Campus/SRO
□ Courts/Jail/Detention/Parole
□ Criminal Investigation/Narcotics
□ Crisis Intervention
□ Crisis Negotiation
□ Dive Team
□ DUI/DWI
□ Equipment/Logistics/Quartermaster
□ Executive Protection
□ Family Support
□ Fugitive Apprehension
□ Gang
□ Harbor Patrol
□ Homeland Defense/Terrorism
□ Homicide
□ Intelligence
□ IT/Technology
□ K-9
□ Motors
□ Mounted Patrol
□ Patrol/Traffic
□ Procurement/Purchasing
□ Recruiting
□ SWAT/SAU/SRT
□ Training Division
□ Vice
□ Not Applicable

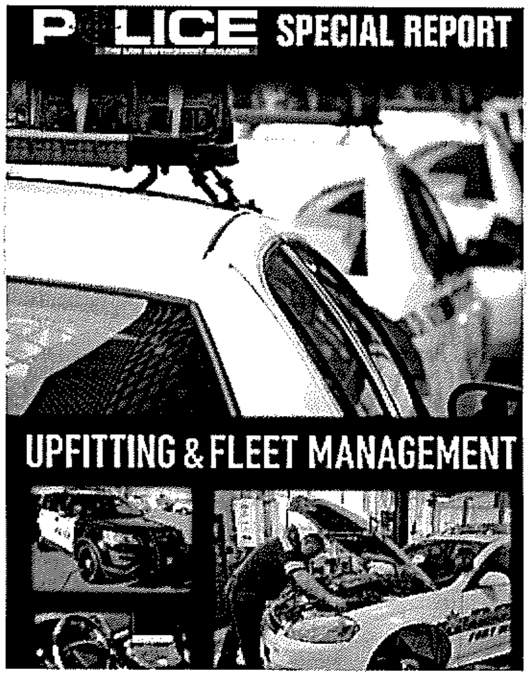
SUBMIT

By filling out this form you consent to Bobit Business Media's privacy policy (http://www.bobitbusinessmedia.com/privacy.aspx) and to receive offers, newsletters and other promotional communications from Bobit Business Media and its trusted partners. You can withdraw consent at any time. You also consent to Bobit Business Media sharing your contact information with the sponsor(s) of the resource so they can contact you directly concerning their product.

MORE

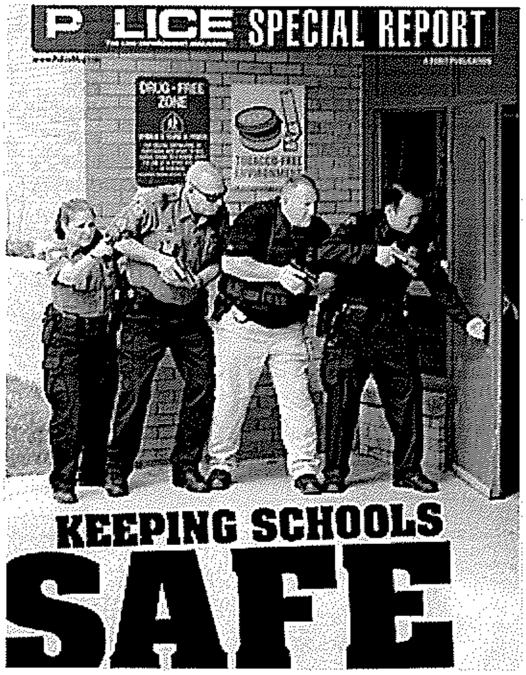
WHITEPAPERS

Host Your Whitepapers (/advertise)



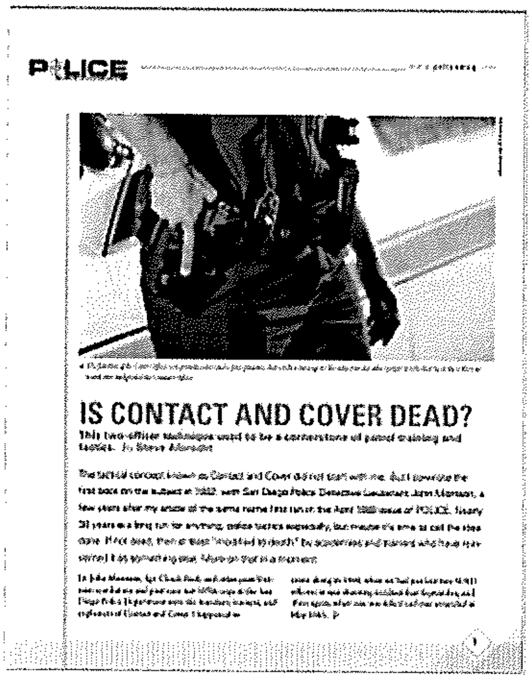
(/vehicle-ops/506764/special-report-upfitting-fleet-management)

Special Report: Upfitting & Fleet Management (/vehicle-ops/506764/special-report-upfitting-fleet-management)



(/technology/424510/special-report-keeping-schools-safe)

Special Report: Keeping Schools Safe (/technology/424510/special-report-keeping-schools-safe)



POLICE

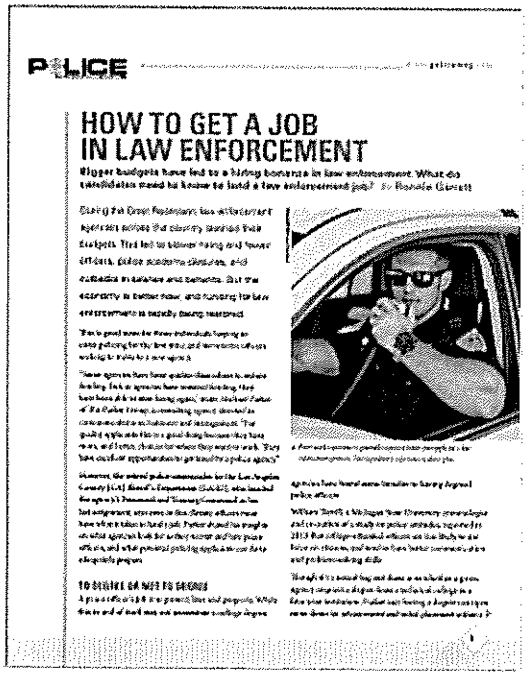
IS CONTACT AND COVER DEAD?

This two-officer technique used to be a cornerstone of patrol training and tactics. By Steve Albrecht

[illegible]

(/procedures-policies/502807/is-contact-and-cover-dead)

Is Contact and Cover Dead? (/procedures-policies/502807/is-contact-and-cover-dead)



POLICE

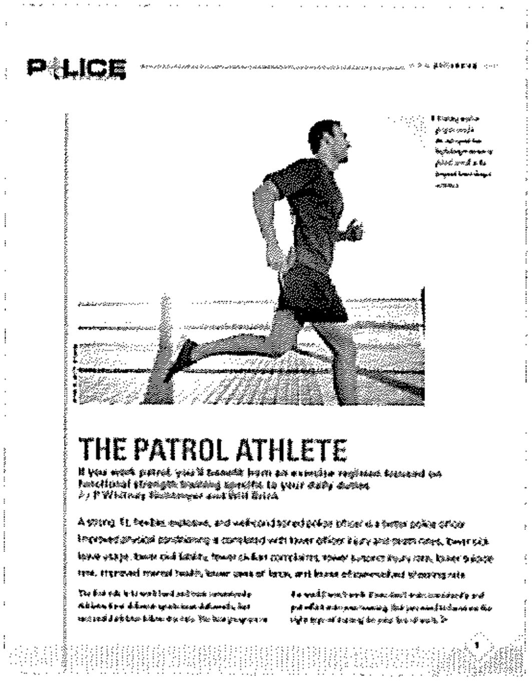
HOW TO GET A JOB IN LAW ENFORCEMENT

Bigger budgets have led to a hiring bonanza in law enforcement. What do candidates need to know to land a law enforcement job? By Ronnie Garrett

[illegible]

(/training-careers/502804/how-to-get-a-job-in-law-enforcement)

How to Get a Job in Law Enforcement (/training-careers/502804/how-to-get-a-job-in-law-enforcement)



POLICE

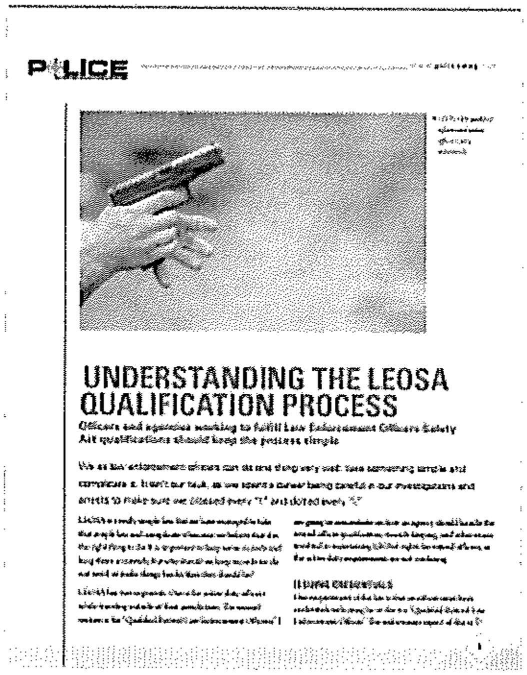
THE PATROL ATHLETE

If you work patrol, you'll benefit from an exercise regimen focused on functional strength training specific to your daily duties

[illegible]

(/patrol/502801/the-patrol-athlete)

The Patrol Athlete (/patrol/502801/the-patrol-athlete)



POLICE

UNDERSTANDING THE LEOSA QUALIFICATION PROCESS

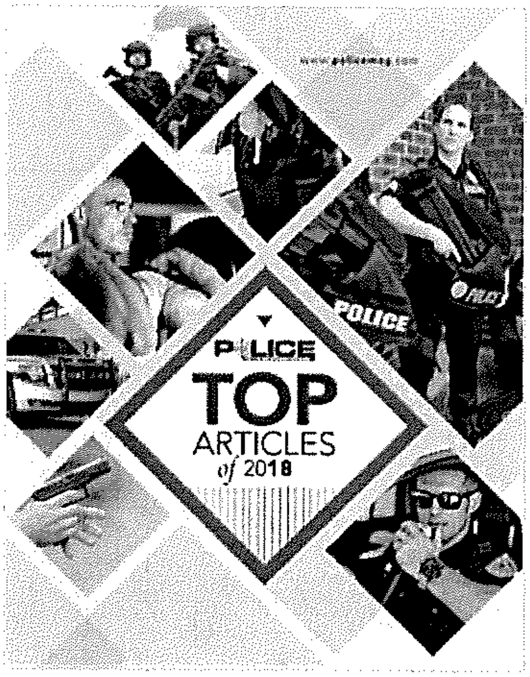
Officers and agencies working to fulfill Law Enforcement Officers Safety Act qualifications should keep the process simple

We as law enforcement officers can do one thing very well: take something simple and complicate it. It isn't our fault, as we spend a career being careful in our investigations and arrests to make sure we crossed every "T" and dotted every "I."

[illegible]

(/procedures-policies/502142/understanding-the-leosa-qualification-process)

Understanding the LEOSA Qualification Process (/procedures-policies/502142/understanding-the-leosa-qualification-process)

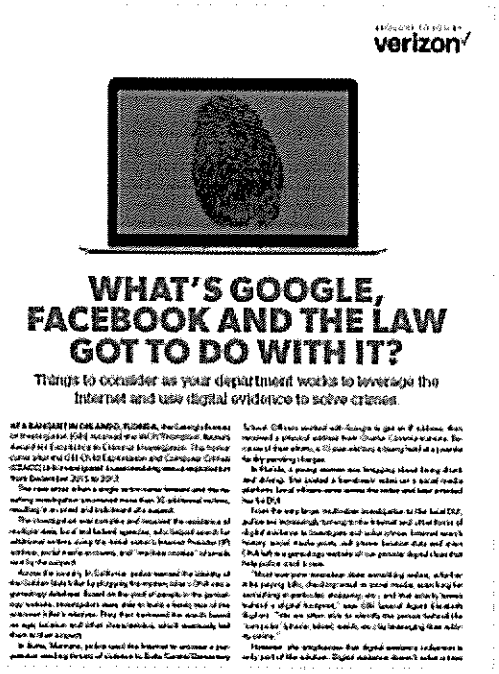


POLICE

TOP ARTICLES of 2018

(/patrol/487148/police-magazine-top-articles-of-2018)

Police Magazine - Top Articles of 2018 (/patrol/487148/police-magazine-top-articles-of-2018)



verizon✓

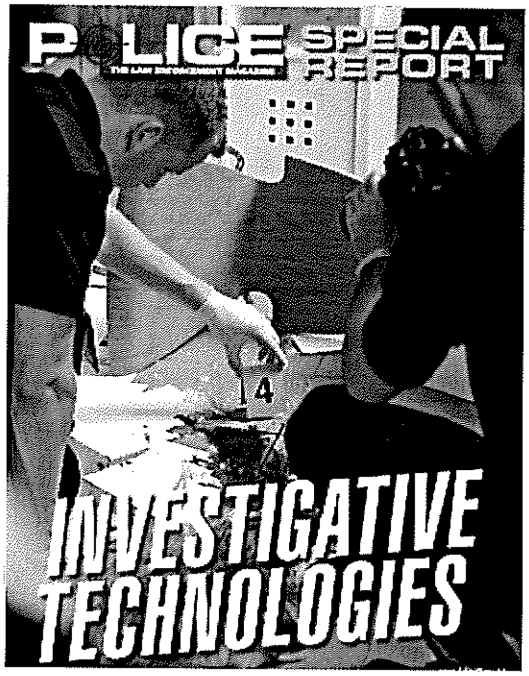
WHAT'S GOOGLE, FACEBOOK AND THE LAW GOT TO DO WITH IT?

Things to consider as your department works to leverage the Internet and use digital evidence to solve crimes.

[illegible]

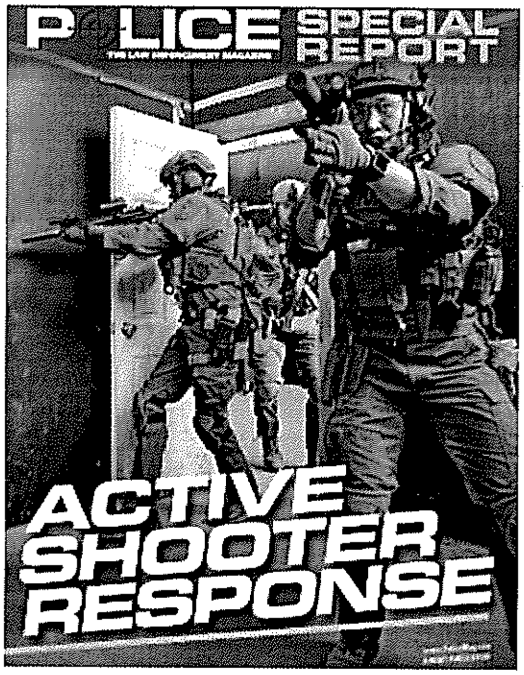
(/technology/424494/whats-google-facebook-and-the-law-got-to-do-with-it)

What's Google, Facebook and the law got to do with it? (/technology/424494/whats-google-facebook-and-the-law-got-to-do-with-it)



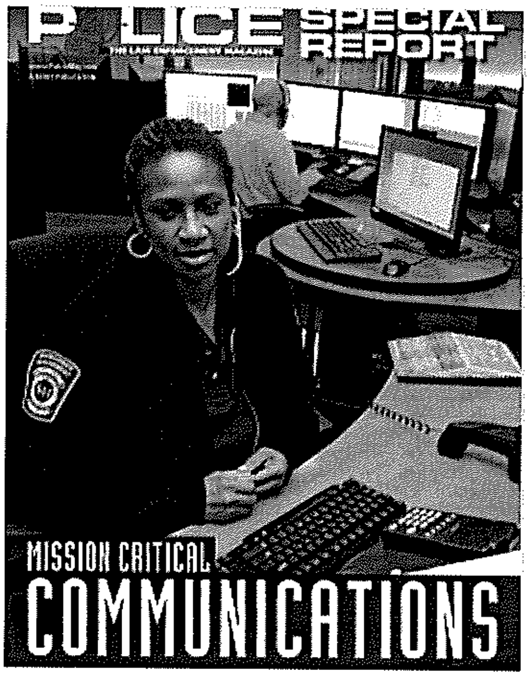
(/technology/424496/special-report-investigative-technologies)

Special Report: Investigative Technologies (/technology/424496/special-report-investigative-technologies)



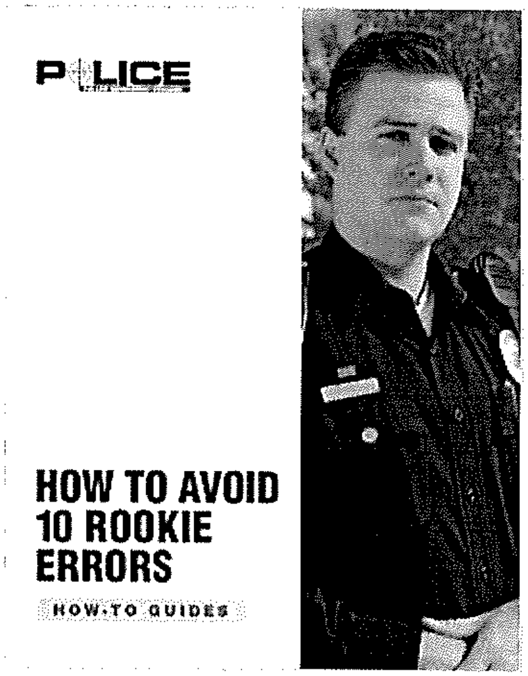
(/training-careers/424498/special-report-active-shooter-response)

Special Report: Active Shooter Response (/training-careers/424498/special-report-active-shooter-response)



(/technology/424500/special-report-mission-critical-communications)

Special Report: Mission Critical Communications (/technology/424500/special-report-mission-critical-communications)



(/training-careers/424502/how-to-avoid-10-rookie-errors)

How To Avoid 10 Rookie Errors (/training-careers/424502/how-to-avoid-10-rookie-errors)

LOAD MORE (/TECHNOLOGY/424550/FACIAL-RECOGNITION-ART-OR-SCIENCE?PAGE=2)

Search (/search) | Menu

News (/news) Photos (/photo-galleries) Blogs (/blogs) Videos (/videos) Cop Slang (/cop-slang)

How-To's (/whitepapers) Magazine (/issues) Products (/products) Jobs (http://policecareerfinder.com/)

Directory (http://directory.policemag.com/) Webinars (/webinars)

Newsletters (https://bob.dragonforms.com/init.do?omedasite=BOB6226_PZpref)

POLICE (/) COMMUNITY FOR COPS

Search SEARCH

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle Ops (/vehicle-op

PATROL

Anonymous Amazon Employee Publishes Op-Ed Opposing Sale of Facial Recognition Tech to Police

October 18, 2018 • by Staff Writer (/authors/504428/staff)

Embed from Getty Images (http://www.gettyimages.com/detail/952605500)

An anonymous employee for tech giant Amazon recently posted an opinion article to Medium (https://medium.com/s/story/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac) in which they argue that the sale of facial recognition software to police is wrong because "the product we're selling is a flawed technology that reinforces existing bias."

In June (https://www.policemag.com/channel/technology/news/2018/06/22/amazon-employees-join-aclu-investors-in-protest-amazon-s-sale-of-tech-to-police.aspx), a group of Amazon employees posted to an internal company Wiki page a letter—later obtained by The Hill (https://thehill.com/business-a-lobbying/393583-amazon-employees-protest-sale-of-facial-recognition-tech-to-law)—asking company executives to discontinue its sale of the company's Rekognition facial recognition software to law enforcement agencies.

The anonymous op-ed published this week rekindles opposition to the sale of that technology to police.

"Amazon, where I work, is currently allowing police departments around the country to purchase its facial recognition product, Rekognition, and I and other employees demand that we stop immediately," the opinion piece reads.

The employee wrote, "Amazon is designing, marketing, and selling a system for dangerous mass surveillance right now," the write states. "Amazon's website brags of the system's ability to store and search tens of millions of faces at a time. Law enforcement has already started using facial recognition with virtually no public oversight or debate or restrictions on use from Amazon."

Read more about Investigations (/tags?tag=Investigations)

Electronic Surveillance (/tags?tag=Electronic+Surveillance)

Facial Recognition (/tags?tag=Facial+Recognition)

Civil Rights Activists (/tags?tag=Civil+Rights+Activists)

Amazon Web Services (/tags?tag=Amazon+Web+Services) patrol (/tags?tag=patrol)

0 Comments

Join the discussion...

MORE

PATROL

NEWS (/NEWS)

Texas Police Officer Struck by Suspected Drunk Driver (/513407/texas-police-officer-struck-by-suspected-drunk-driver)

An officer with the San Marcos (TC) Police Department was severely injured when she was struck by a vehicle on Saturday night.

NEWS (/NEWS)

Detroit Police Officer Recovering After Being Shot (/513406/detroit-police-officer-recovering-after-being-shot)

An officer with the Detroit Police Department is recovering after being shot Saturday

OFFICER FAVORITES (/ISSUES)

- Tactical Gear (https://www.policemag.com/tag tag=Tactical+Gear)
- How-to Guides (https://www.policemag.com/tag tag=How-To+Guides)
- Officer Fitness (https://www.policemag.com/tag tag=Officer+Fitness)

trying to stop a speeding driver on Saturday night.

NEWS (/NEWS)

Kentucky Officer Struck By Car While Investigating Vehicle Break-In (/513405/kentucky-officer-struck-by-car-while-investigating-vehicle-break-in)

An officer with the Louisville Metro Police Department was injured after being hit by a vehicle early Sunday morning.

NEWS (/NEWS)

Illinois Man in Custody Fires Gun Inside Police Department (/513404/illinois-man-in-custody-fires-gun-inside-police-department)

A man arrested for suspected theft and battery drew a gun inside the Carbondale (IL) Police Department and opened fire.

NEWS (/NEWS)

Georgia Officer Delivers Baby at Gas Station (/513403/georgia-officer-delivers-baby-at-gas-station)

An officer with the Hazlehurst (GA) Police Department was called to a local gas station to assist in the delivery of a baby boy late last week.

NEWS (/NEWS)

- Drug Cartels (https://www.policemag.com/tag tag=drug+cartels)
- Stupid Criminals (https://www.policemag.com/tag tag=Stupid+Criminals)
- Shots Fired (https://www.policemag.com/tag tag=Shots+Fired)
- Police Humor (https://www.policemag.com/tag tag=Police+Humor)
- Defensive Tactics (https://www.policemag.com/tag tag=Defensive+Tactics)

COP SLANG (HTTPS://POLICEMAG.COM/COP-SLANG)

Top Terms (https://policema slang)

(https://policemag.cc slang)

Badge Bunny (https://www.police slang/badge-bunny)
Blue Falcon (https://policemag.co slang/blue-falcon)
Lot Lizard (https://policemag.com/cop-slang/lot-lizard)

Zebra (https://www.policemag.com/cop slang/zebra)
Personal (https://polic slang/persor
Vox (https://polic slang/vox)

VIEW TERMS (HTTPS://POLICEMAG.C

✉ Newsletter

Proposed Massachusetts Bill Would Impose Death Penalty for Cop Killers (/513402/proposed-massachusetts-bill-would-impose-death-penalty-for-cop-killers)

According to Fox News, the proposed legislation would give judges the option of sentencing people over 18 to death for killing a police officer.

NEWS (/NEWS)

Connecticut Officer Saves Couple from Burning Home (/513401/connecticut-officer-saves-couple-from-burning-home)

An officer with the Shelton (CT) Police Department has been credited with saving the lives of a couple whose home suffered extensive damage from an early-morning fire.

NEWS (/NEWS)

Suspect in Killing of AL Officer Captured (/513346/suspect-in-killing-of-al-officer-captured)

Auburn police say the three officers were responding to a domestic disturbance call about 10 p.m. When they arrived on the scene they were reportedly fired upon by the suspect, identified as Wilkes.

NEWS (/NEWS)

AL Officer Killed—2 Wounded, Suspect at Large (/513338/al-officer-killed2-wounded-suspect-at-large)

The three officers were shot late Sunday night at a mobile home park in Auburn and a manhunt is underway for a suspect wearing body armor. One of the other two wounded officers is in critical condition. Both are expected to survive.

NEWS (/NEWS)

Tourniquet, Ballistic Vest Save Life of Oregon Officer After Being Shot (/513181/tourniquet-ballistic-vest-save-life-of-oregon-officer-after-being-shot)

Email Address SUBMIT

MAGAZINE (/ISSUES)

January 2019

Digital Edition (/digitalmagazine)
Digital Archives (/digitalarchives)
Subscribe (/subscribe)

(/513181/tourniquet-ballistic-vest-save-life-of-oregon-officer-after-being-shot)
An officer with the Salem (OR) Police Department is recovering after being shot several times during a traffic stop on Tuesday night.

LOAD MORE (/362596/ANONYMOUS-AMAZON-EMPLOYEE-PUBLISHES-OP-ED-OPPOSING-

Don't Miss Another Story

Email Address SUBMIT

Topics

Training & Careers (/training-careers)
Special Units (/special-units)
Patrol (/patrol)
Technology (/technology)
Vehicle Ops (/vehicle-ops)
Weapons (/weapons)
Point of Law (/point-of-law)
Procedures & Policies (/procedures-policies)
Investigations (/investigations)
Command (/command)

Essentials

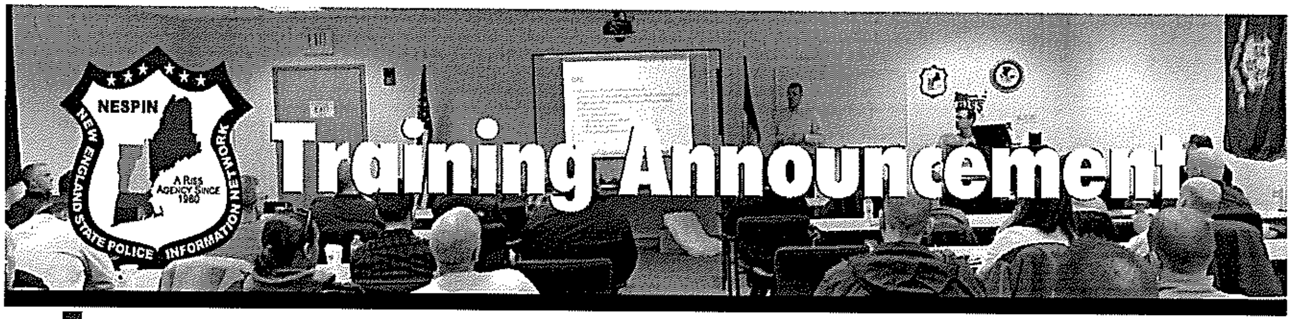
News (/news)
Photos (/photo-galleries)
Videos (/videos)
Blogs (/blogs)
How-To's (/whitepapers)
Magazine (/issues)
Products (/products)
Jobs (http://policecareerfind

Services

Subscription (/subscribe)
Advertise (/advertise)
Contact Us (/contact-us)
Online Store (http://store.policemag.com/)
Privacy Policy (https://www.bobitbusinessmedia.com/privac policy/)
Newsletter Sign Up

Connect

(https://bob.dragonforms.com/init.do?
omedasite=BOB6226_PZpref)
Suppliers
Directory
(http://directory.policemag.com/?
ref=ftr)



IMPOSTOR ANALYSIS 101

GENERATING INVESTIGATIVE LEADS ONCE YOU'VE ID AN IMPOSTOR

NO COST FOR THIS TRAINING

DECEMBER 10, 2018

LOCATION:Â NESPIN 124 GROVE ST, FRANKLIN MA.

IMPOSTOR ANALYSIS 101
GENERATING INVESTIGATIVE LEADS ONCE YOU'VE ID AN IMPOSTOR
NO COST FOR THIS TRAINING
DECEMBER 10, 2018

This one-day course will teach participants how to leverage available information to generate investigative leads in an identity theft case. Youâ€™ve identified the impostor, but there are still a number of steps between you and a successful prosecution. Learn how to prepare a solid case presentation that any prosecutor would appreciate.
Participants will also be treated to brief presentation of authentic versus counterfeit federal documents and how to tell them apart at this courseâ€™s conclusion.

Course Topics include:
ï‚· Behavioral Biometrics â€“ Handwriting & Signature
ï‚· Facial Recognition
ï‚· Forensic Statement Analysis
ï‚· Deceased Identities
ï‚· Jail & Prison information
ï‚· Social Media Analysis
ï‚· Charge stacking
ï‚· Consular records
ï‚· Case Preparation and Analysis Tools
ï‚· Federal Document Authenticity with live samplesÂ

Please go to the following link for complete details and registration information:

https://extranet.riss.net/public/1412a1e9-0aa9-45b2-822c-dbd15ccf7c56

Please do not reply to this e-mail as it is an unmonitored alias.
If you do not wish to receive these training mailings, please choose the Opt-out feature at the bottom of this email.

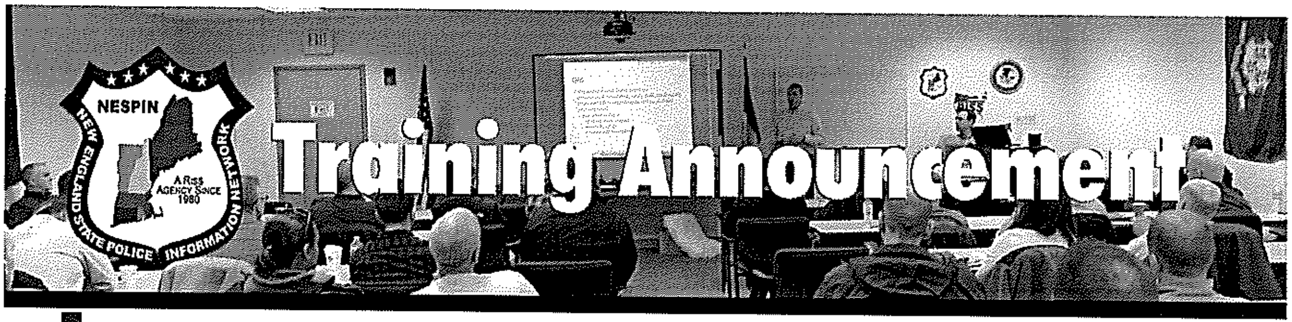
Share this email:

Manage your preferences | **Opt out** using **TrueRemoveâ„¢**
Got this as a forward? **Sign up** to receive our future emails.
View this email **online.**

124 Grove Street Suite 105
Franklin, MA | 02038 US

This email was sent to rpowers@northamptonma.gov.
To continue receiving our emails, add us to your address book.

emma



THIS CLASS IS NOW FULL!!!!!!!!!

IMPOSTOR ANALYSIS 101

GENERATING INVESTIGATIVE LEADS ONCE YOU'VE ID AN IMPOSTOR

NO COST FOR THIS TRAINING

DECEMBER 10, 2018

LOCATION:Â NESPIN 124 GROVE ST, FRANKLIN MA.

THIS CLASS IS NOW FULL!!!!!!!!

IMPOSTOR ANALYSIS 101
GENERATING INVESTIGATIVE LEADS ONCE YOU'VE ID AN IMPOSTOR
NO COST FOR THIS TRAINING
DECEMBER 10, 2018

This one-day course will teach participants how to leverage available information to generate investigative leads in an identity theft case. Youâ€™ve identified the impostor, but there are still a number of steps between you and a successful prosecution. Learn how to prepare a solid case presentation that any prosecutor would appreciate.
Participants will also be treated to brief presentation of authentic versus counterfeit federal documents and how to tell them apart at this courseâ€™s conclusion.

Course Topics include:
ï‚· Behavioral Biometrics â€“ Handwriting & Signature
ï‚· Facial Recognition
ï‚· Forensic Statement Analysis
ï‚· Deceased Identities
ï‚· Jail & Prison information
ï‚· Social Media Analysis
ï‚· Charge stacking

ï‚· Consular records
ï‚· Case Preparation and Analysis Tools
ï‚· Federal Document Authenticity with live samplesÂ

Please go to the following link for complete details and registration information:

https://extranet.riss.net/public/1412a1e9-0aa9-45b2-822c-dbd15ccf7c56

Please do not reply to this e-mail as it is an unmonitored alias.
If you do not wish to receive these training mailings, please choose the Opt-out feature at the bottom of this email.

Share this email:

Manage your preferences | **Opt out** using **TrueRemoveâ„¢**
Got this as a forward? **Sign up** to receive our future emails.
View this email **online**.

124 Grove Street Suite 105
Franklin, MA | 02038 US

This email was sent to rpowers@northamptonma.gov.
To continue receiving our emails, add us to your address book.

emma

POLICE THE LAW ENFORCEMENT MAGAZINE (/)

Search Menu

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle O

TECHNOLOGY

UK Police Testing Facial Recognition Software on Holiday Shoppers

December 19, 2018 • by Staff Writer (/authors/504428/staff)

Embed from Getty Images (http://www.gettyimages.com/detail/905553688)

Police in London are testing facial recognition software on Christmas shoppers, hoping the technology will detect known and wanted criminals in the crowds.

According to The Verge (https://www.theverge.com/2018/12/18/18146083/facial-recognition-police-london-uk-met-christmas-shopping)—a website that reports on cutting edge technology—this week's experiment is the seventh time the Metropolitan Police Department has tested facial recognition in public. The technology has previously been used at large events, including the Notting Hill Carnival in 2016 and 2017, and Remembrance Day services last year.

The Verge reports that the cameras will be attached to lampposts or mounted on vehicles. The department is using software developed by Japanese firm NEC that measures different facial features such as the distance between the eyes and the length and angle of the nose. The scan is then compared to a database of police mugshots.

Critics of the technology have said that it is not yet advanced enough to be trusted for accuracy, noting that "false positives" can result from a variety of factors such as poor lighting.

Read more about International Agencies (/tags?tag=International+Agencies)

Facial Recognition (/tags?tag=Facial+Recognition) technology (/tags?tag=technology)

0 Comments

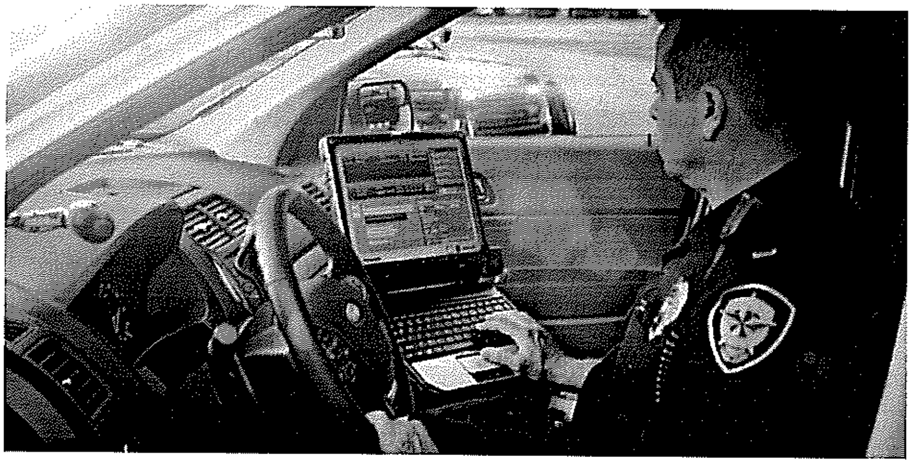
Join the discussion...

MORE

TECHNOLOGY

NEWS (/NEWS)

Panasonic to Take Part in Panel at IACP Technology Conference (/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)



(/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)

The IACP Technology Conference is taking place in Jacksonville, FL, May 20–22. At the event on Tuesday, May 21, at 4 pm ET, Panasonic will take part in the panel discussion, "Managing Officer Safety Now and in the Future through a Strong Technology Ecosystem."

NEWS (/NEWS)

Video: Could a Robot Make Traffic Stops Safer? (/512502/video-could-a-robot-make-traffic-stops-safer)

(/512502/video-could-a-robot-make-traffic-stops-safer)

Once the officer's vehicle is parked behind the motorist's car, GoBetween rolls up to the driver's side window of the motorist, where it becomes the officer's eyes, ears and mouth. A spike strip automatically placed in front of the car's rear wheels keeps the motorist from driving away until the traffic stop is completed.

NEWS (/NEWS)

Knightscope Adds Facial Recognition to K1 Security Robots

(/512416/knightscope-adds-facial-recognition-to-k1-security-robots)

"Prospective clients were able to upload a photo into the Knightscope Security Operations Center (KSOC) and then watch the K1 detect and report them as they moved about the booth. One creative individual even attempted to elude 'capture' by donning a pair of dark sunglasses to no avail," the company says.

NEWS (/NEWS)

Gamber-Johnson Wins WI Governor's Export Achievement Award (/512377/gamber-johnson-wins-wi-governors-export-achievement-award)

Gamber-Johnson has been named the recipient of the 2019 Governor's Export Achievement Award by the Wisconsin Economic Development Corporation (WEDC) for its contribution to Wisconsin's exporting strength.

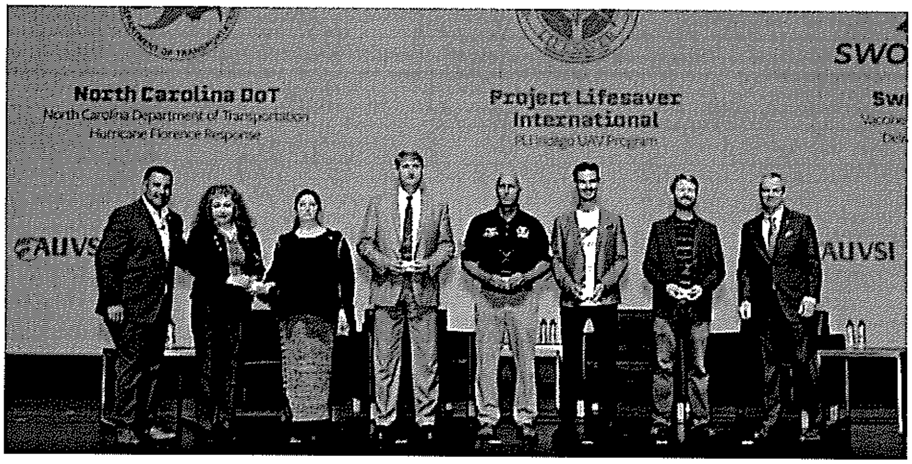
NEWS (/NEWS)

San Francisco Could Ban Use of Facial Recognition by Law Enforcement (/512178/san-francisco-could-ban-use-of-facial-recognition-by-law-enforcement)

The proposal, introduced by San Francisco Supervisor Aaron Peskin, would also require public input and the supervisors' approval before agencies buy investigative technology with public funds. That includes the purchase of license plate readers, toll readers, closed-circuit cameras, body cams, and biometrics technology and software for forecasting criminal activity.

NEWS (/NEWS)

Project Lifesaver International Receives Prestigious International Humanitarian Award (/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

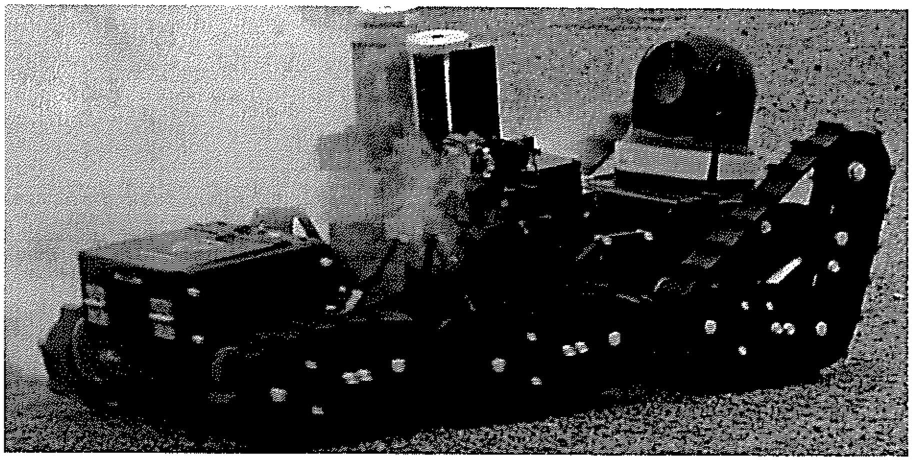

North Carolina DoT
North Carolina Department of Transportation
Hurricane Florence Response
Project Lifesaver International
AUVSI
AUVSI
SWO

(/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

Project Lifesaver International (PLI) has been awarded the Humanitarian Xcellence Award by the Association for Unmanned Vehicles Systems International for its use of DJI drones to locate missing persons.

NEWS (/NEWS)

Transcend Tactical Introduces Mobile Gas Deployment System for Robots (/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)



(/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

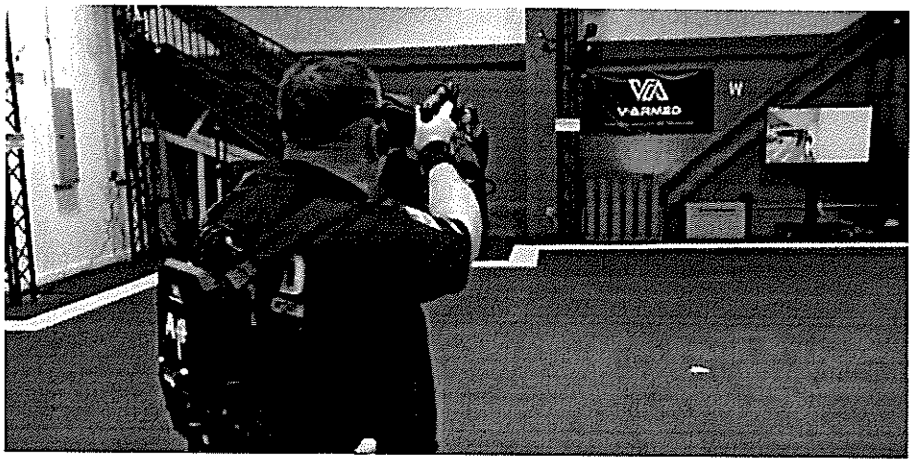
Transcend Tactical has launched a gas deployment system that can be added to its Vantage robot to deploy two hot or cold gas grenades remotely and with mobility.

The Role of Data Analytics in Intelligence-Led Policing (/511412/the-role-of-data-analytics-in-intelligence-led-policing)

An agency's data is only as good as what it allows them to do next. Public safety agencies can increase situational awareness and decrease crime in the community by utilizing data analytics to the fullest extent.

NEWS (/NEWS)

NYPD Testing Virtual Reality-Based Training (/511543/nypd-testing-virtual-reality-based-training)



(/511543/nypd-testing-virtual-reality-based-training)

The NYPD is testing a virtual reality scenario-based training system. About 200 officers participated in the training program, which was conducted earlier this month at a state-of-the-art facility in Williamsburg, Brooklyn.

NEWS (/NEWS)

Axon Develops Tool for Measuring Officer Performance and Identifying Training Needs Through Body Camera Footage (/511538/axon-develops-tool-for-measuring-officer-performance-and-identifying-training-ne)

Axon has announced the launch of Axon Performance, a data analytics tool that helps to streamline the policy review process for law enforcement agencies. Axon Performance allows supervisors to more efficiently review video footage, perform agencywide officer performance evaluations, identify training needs and save officers time so they can spend more time in their communities.

LOAD MORE (/499834/UK-POLICE-TESTING-FACIAL-RECOGNITION-SOFTWARE-ON-HOLIDAY-SHOPPERS?PAGE=2)

Search (/search) | ☰ Menu

POLICE THE LAW ENFORCEMENT MAGAZINE (/)

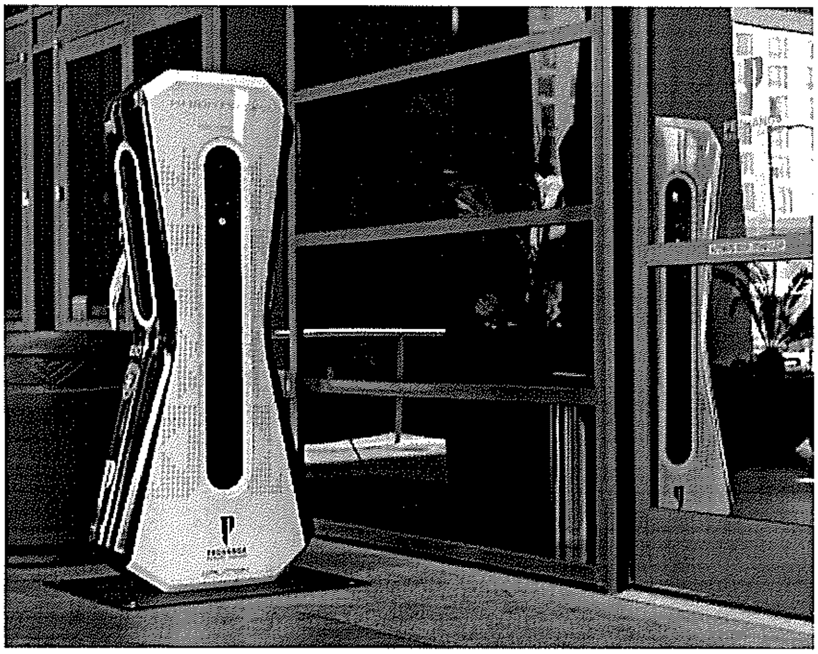
Search Menu

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technolog

TECHNOLOGY

Knightscope Adds Facial Recognition to K1 Security Robots

May 10, 2019 • by Staff Writer (/authors/504428/staff)



Knightscope K1 with new facial recognition technology outside Pechanga Resort Casino. (Photo: Business Wire)

Knightscope (https://www.knightscope.com/)has announced the beta release of a facial recognition feature for its K1 security robot. The announcement was made in March at the International Security Conference & Exhibition (ISC West) in Las Vegas.

The facial recognition tool was developed by Knightscope working with one of its clients, Pechanga Resort Casino in Temecula, CA. The software works on the company's K1 security robot and utilizes deep learning to detect, analyze, and compare faces and help enhance Workplace Violence Prevention (WVP) programs.

"Demonstration of the new feature helped make this year's ISC West one of the busiest and most successful trade shows for Knightscope to date. Prospective clients were able to upload a photo into the Knightscope Security Operations Center (KSOC) and then watch the K1 detect and report them as they moved about the booth. One creative individual even attempted to elude 'capture' by donning a pair of dark sunglasses to no avail," the company says.

"While facial recognition is largely seen as a tool to protect against known threats, it is also capable of greeting VIPs with a personal message and notifying our clients of VIP arrivals on site. It's a great way for businesses to think outside the box to deliver a greater return on their security investment," the company added.

Read more about Knightscope (/tags?tag=Knightscope) Robots (/tags?tag=Robots) Facial Recognition (/tags?tag=Facial+Recognition)

0 Comments

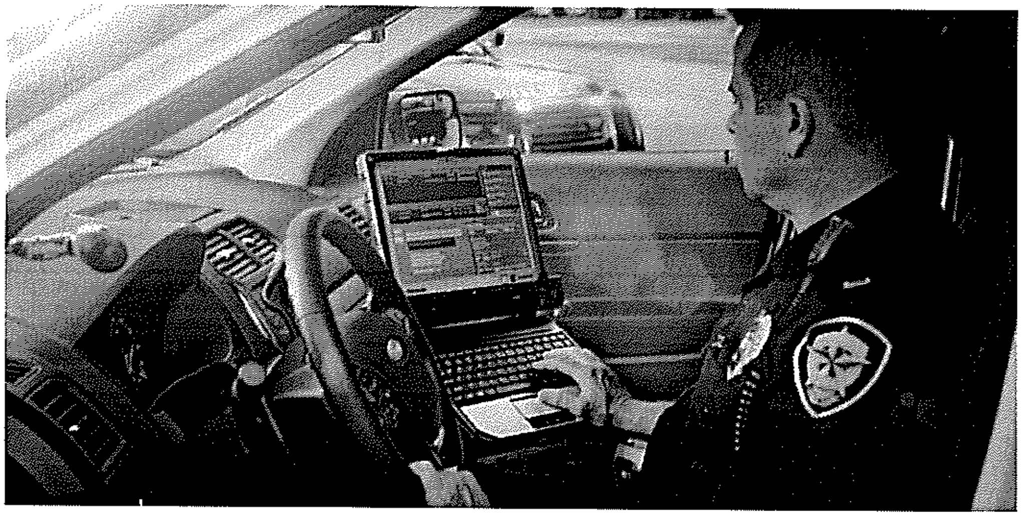
Join the discussion...

MORE

TECHNOLOGY

NEWS (/NEWS)

Panasonic to Take Part in Panel at IACP Technology Conference (/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)



(/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)

The IACP Technology Conference is taking place in Jacksonville, FL, May 20–22. At the event on Tuesday, May 21, at 4 pm ET, Panasonic will take part in the panel discussion, "Managing Officer Safety Now and in the Future through a Strong Technology Ecosystem."

NEWS (/NEWS)

Video: Could a Robot Make Traffic Stops Safer? (/512502/video-could-a-robot-make-traffic-stops-safer)

(/512502/video-could-a-robot-make-traffic-stops-safer)

Once the officer's vehicle is parked behind the motorist's car, GoBetween rolls up to the driver's side window of the motorist, where it becomes the officer's eyes, ears and mouth. A spike strip automatically placed in front of the car's rear wheels keeps the motorist from driving away until the traffic stop is completed.

NEWS (/NEWS)

Gamber-Johnson Wins WI Governor's Export Achievement Award (/512377/gamber-johnson-wins-wi-governors-export-achievement-award)

Gamber-Johnson has been named the recipient of the 2019 Governor's Export Achievement Award by the Wisconsin Economic Development Corporation (WEDC) for its contribution to Wisconsin's exporting strength.

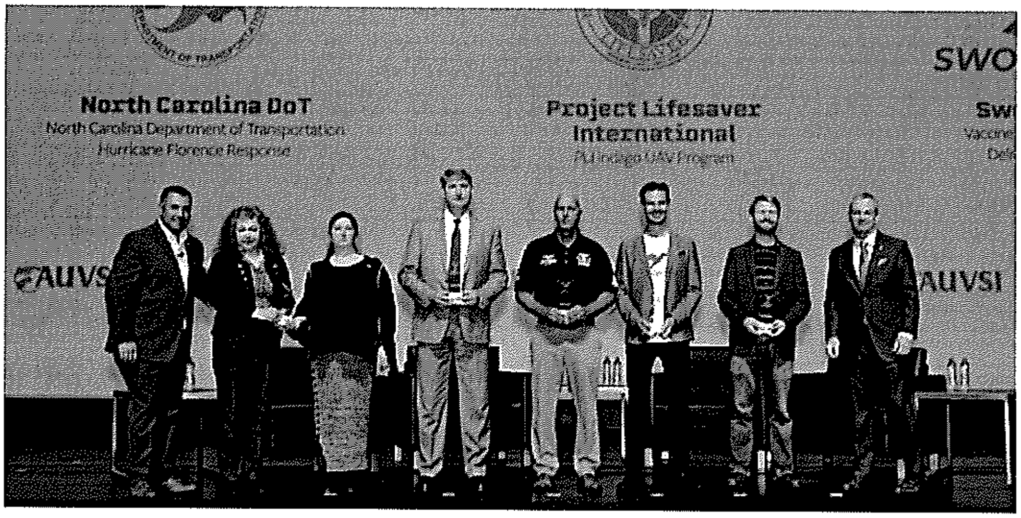
NEWS (/NEWS)

San Francisco Could Ban Use of Facial Recognition by Law Enforcement (/512178/san-francisco-could-ban-use-of-facial-recognition-by-law-enforcement)

The proposal, introduced by San Francisco Supervisor Aaron Peskin, would also require public input and the supervisors' approval before agencies buy investigative technology with public funds. That includes the purchase of license plate readers, toll readers, closed-circuit cameras, body cams, and biometrics technology and software for forecasting criminal activity.

NEWS (/NEWS)

Project Lifesaver International Receives Prestigious International Humanitarian Award (/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

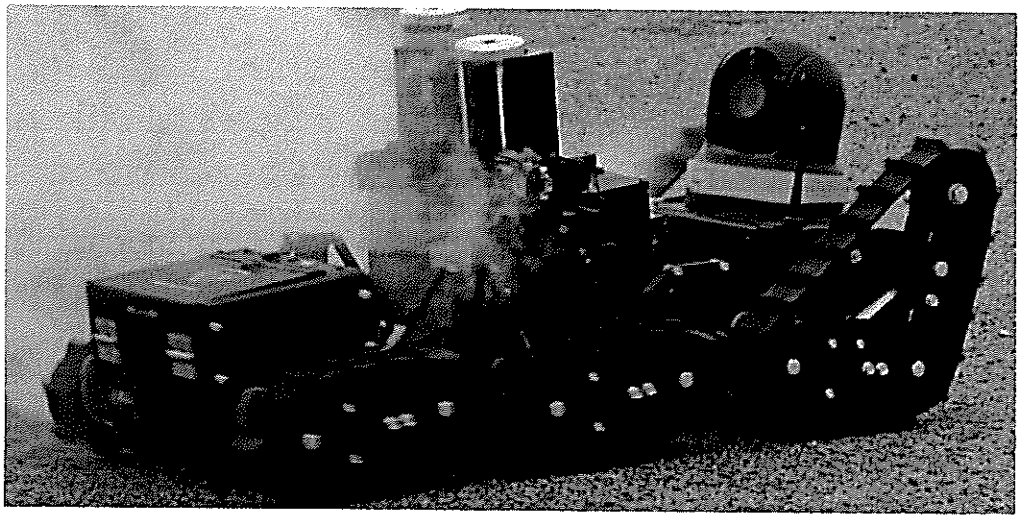

North Carolina DoT
North Carolina Department of Transportation
Hurricane Florence Response
Project Lifesaver International
PLI Indago UAV Program
SWO
AUVSI
AUVSI

(/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

Project Lifesaver International (PLI) has been awarded the Humanitarian Xcellence Award by the Association for Unmanned Vehicles Systems International for its use of DJI drones to locate missing persons.

NEWS (/NEWS)

Transcend Tactical Introduces Mobile Gas Deployment System for Robots (/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

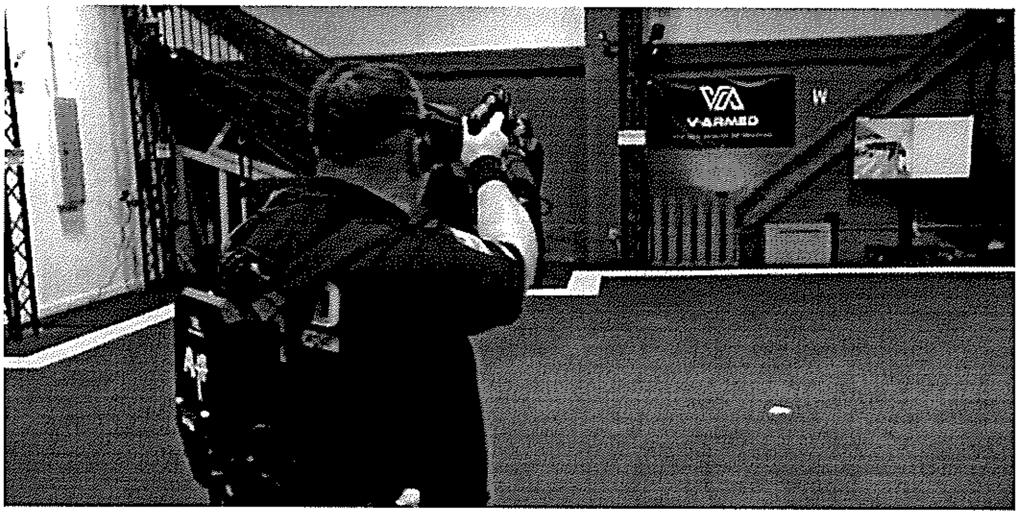


(/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

Transcend Tactical has launched a gas deployment system that can be added to its Vantage robot to deploy two hot or cold gas grenades remotely and with mobility.

NEWS (/NEWS)

NYPD Testing Virtual Reality-Based Training (/511543/nypd-testing-virtual-reality-based-training)



(/511543/nypd-testing-virtual-reality-based-training)

The NYPD is testing a virtual reality scenario-based training system. About 200 officers participated in the training program, which was conducted earlier this month at a state-of-the-art facility in Williamsburg, Brooklyn.

NEWS (/NEWS)

Axon Develops Tool for Measuring Officer Performance and Identifying Training Needs Through Body Camera Footage (/511538/axon-develops-tool-for-measuring-officer-performance-and-identifying-training-ne)

Axon has announced the launch of Axon Performance, a data analytics tool that helps to streamline the policy review process for law enforcement agencies. Axon Performance allows supervisors to more efficiently review video footage, perform agencywide officer performance evaluations, identify training needs and save officers time so they can spend more time in their communities.

NEWS (/NEWS)

Axon Launches First Advanced AI-Powered Redaction Tool (/511537/axon-launches-first-advanced-ai-powered-redaction-tool)

Axon has announced the launch of Redaction Assistant, the first advanced artificial intelligence (AI) powered tool to be offered to law enforcement agencies and prosecutors through the Axon network. Redaction Assistant is a productivity tool built to increase efficiency for agencies who currently spend up to eight hours manually redacting each hour of body camera video footage.

LOAD MORE (/512416/KNIGHTSCOPE-ADDS-FACIAL-RECOGNITION-T

Search (/search) | ☰ Menu

POLICE (/)
THE LAW ENFORCEMENT MAGAZINE

Search Menu

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle Ops (

TECHNOLOGY

San Francisco Could Ban Use of Facial Recognition by Law Enforcement

May 7, 2019 • by Staff Writer (/authors/504428/staff)

San Francisco could become the first city in the nation to ban any city department from using facial recognition under a proposal that says any benefits of the technology do not outweigh its impact on civil rights.

The San Francisco Board of Supervisors committee is scheduled to vote Monday on the Stop Secret Surveillance Ordinance, which would make it illegal for any department to "obtain, retain, access or use" any face-recognition technology or information obtained from such technology.

The proposal, introduced by San Francisco Supervisor Aaron Peskin in January, would also require public input and the supervisors' approval before agencies buy investigative technology with public funds. That includes the purchase of license plate readers, toll readers, closed-circuit cameras, body cams, and biometrics technology and software for forecasting criminal activity, the San Jose Mercury (https://www.mercurynews.com/2019/05/06/san-francisco-oakland-could-be-first-cities-in-nation-to-ban-facial-recognition/) reports.

Other Bay Area cities and counties, including Berkeley, Palo Alto and Santa Clara County, have similar rules in place about buying investigative technology, but a San Francisco ban on facial recognition would set a precedent. In Oakland, a proposal to add a ban on facial recognition to city regulations is set to be considered by Oakland's Public Safety Committee later this month.

The San Francisco Police Department, which said it doesn't use facial recognition, submitted amendments to the ordinance after talking with other city departments, community groups, neighborhood watch groups, and businesses.

Lee Hepner, legislative aide to Peskin, said the supervisor's office incorporated some of the SFPD's requests into the ordinance. If it is approved in committee Monday, the full board will vote May 14.

Read more about California agencies (/tags?tag=California+agencies) California (/tags?tag=California) Facial Recognition (/tags?tag=Facial+Recognition) ALPR/LPR (/tags?tag=ALPR%2fLPR) Predictive Policing (/tags?tag=Predictive+Policing) Body-Worn Cameras (/tags?tag=Body-Worn+Cameras) the west (/tags?tag=the+west) Anti-Police Activists (/tags?tag=Anti-Police+Activists) ACLU (/tags?tag=ACLU)

0 Comments

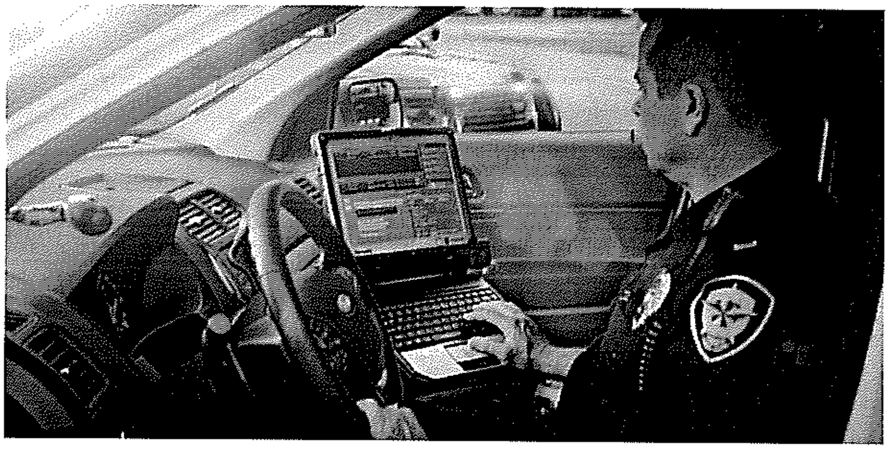
Join the discussion...

MORE

TECHNOLOGY

NEWS (/NEWS)

Panasonic to Take Part in Panel at IACP Technology Conference (/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)



(/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)

The IACP Technology Conference is taking place in Jacksonville, FL, May 20–22. At the event on Tuesday, May 21, at 4 pm ET, Panasonic will take part in the panel discussion, "Managing Officer Safety Now and in the Future through a Strong Technology Ecosystem."

NEWS (/NEWS)

Video: Could a Robot Make Traffic Stops Safer? (/512502/video-could-a-robot-make-traffic-stops-safer)

(/512502/video-could-a-robot-make-traffic-stops-safer)

Once the officer's vehicle is parked behind the motorist's car, GoBetween rolls up to the driver's side window of the motorist, where it becomes the officer's eyes, ears and mouth. A spike strip automatically placed in front of the car's rear wheels keeps the motorist from driving away until the traffic stop is completed.

NEWS (/NEWS)

Knightscope Adds Facial Recognition to K1 Security Robots (/512416/knightscope-adds-facial-recognition-to-k1-security-robots)

"Prospective clients were able to upload a photo into the Knightscope Security Operations Center (KSOC) and then watch the K1 detect and report them as they moved about the booth. One creative individual even attempted to elude 'capture' by donning a pair of dark sunglasses to no avail," the company says.

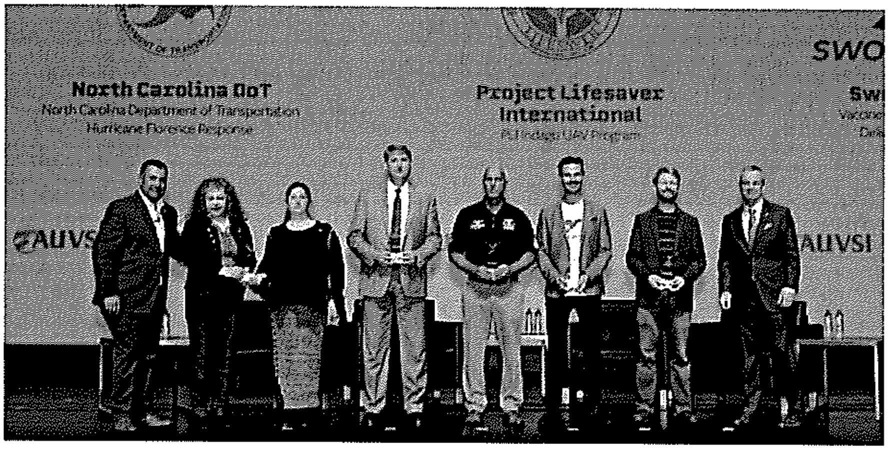
NEWS (/NEWS)

Gamber-Johnson Wins WI Governor's Export Achievement Award (/512377/gamber-johnson-wins-wi-governors-export-achievement-award)

Gamber-Johnson has been named the recipient of the 2019 Governor's Export Achievement Award by the Wisconsin Economic Development Corporation (WEDC) for its contribution to Wisconsin's exporting strength.

NEWS (/NEWS)

Project Lifesaver International Receives Prestigious International Humanitarian Award (/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

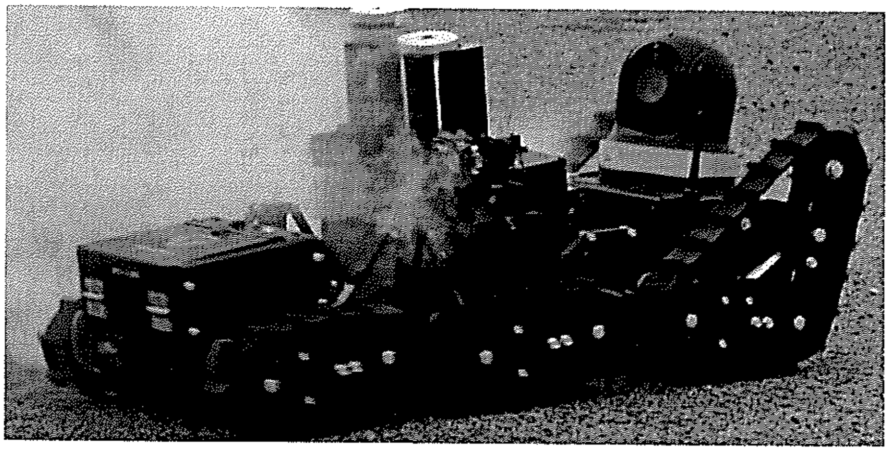

North Carolina DoT
North Carolina Department of Transportation
Hurricane Florence Response
Project Lifesaver International
SWO
AUVSI
AUVSI

(/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

Project Lifesaver International (PLI) has been awarded the Humanitarian Xcellence Award by the Association for Unmanned Vehicles Systems International for its use of DJI drones to locate missing persons.

NEWS (/NEWS)

Transcend Tactical Introduces Mobile Gas Deployment System for Robots (/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)



(/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

Transcend Tactical has launched a gas deployment system that can be added to its Vantage robot to deploy two hot or cold gas grenades remotely and with mobility.

SPONSORED BY MOTOROLA SOLUTIONS

The Role of Data Analytics in Intelligence-Led Policing (/511412/the-role-of-data-analytics-in-intelligence-led-policing)

An agency's data is only as good as what it allows them to do next. Public safety agencies can increase situational awareness and decrease crime in the community by utilizing data analytics to the fullest extent.

NEWS (/NEWS)

NYPD Testing Virtual Reality-Based Training (/511543/nypd-testing-virtual-reality-based-training)

(/511543/nypd-testing-virtual-reality-based-training)

The NYPD is testing a virtual reality scenario-based training system. About 200 officers participated in the training program, which was conducted earlier this month at a state-of-the-art facility in Williamsburg, Brooklyn.

NEWS (/NEWS)

Axon Develops Tool for Measuring Officer Performance and Identifying Training Needs Through Body Camera Footage (/511538/axon-develops-tool-for-measuring-officer-performance-and-identifying-training-ne)

Axon has announced the launch of Axon Performance, a data analytics tool that helps to streamline the policy review process for law enforcement agencies. Axon Performance allows supervisors to more efficiently review video footage, perform agencywide officer performance evaluations, identify training needs and save officers time so they can spend more time in their communities.

NEWS (/NEWS)

Axon Launches First Advanced AI-Powered Redaction Tool (/511537/axon-launches-first-advanced-ai-powered-redaction-tool)

Axon has announced the launch of Redaction Assistant, the first advanced artificial intelligence (AI) powered tool to be offered to law enforcement agencies and prosecutors through the Axon network. Redaction Assistant is a productivity tool built to increase efficiency for agencies who currently spend up to eight hours manually redacting each hour of body camera video footage.

LOAD MORE (/512178/SAN-FRANCISCO-COULD-BAN-USE-OF-FACIAL-RECOGNI

Search (/search) | Menu

POLICE (/)
THE LAW ENFORCEMENT MAGAZINE

Search Menu

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle Ops (/vel

TECHNOLOGY

Lawmaker Asks DOJ to Probe Police Use of Facial Recognition Technology

August 20, 2018 • by Staff Writer (/authors/504428/staff)

Embed from Getty Images (http://www.gettyimages.com/detail/151296068)

Representative Emanuel Cleaver (D-Mo.) has asked the Department of Justice to examine how law enforcement agencies use facial recognition software, saying that he fears the technology has the potential to "exacerbate and entrench" racial divisions in policing practice due to differing performance in matching people from different demographics, according to BiometricUpdate (https://www.biometricupdate.com/201808/u-s-house-rep-calls-on-doj-to-investigate-law-enforcement-use-of-facial-recognition).

In a letter (https://www.scribd.com/document/386360894/Frt-Doj-Letter) to acting Assistant Attorney General John Gore — who leads DOJ's Civil Rights Division — Cleaver said that "if not appropriately implemented, use of the technology may threaten the life and liberty of Americans with crushing force."

Cleaver wrote further that there is "a growing body of evidence" that suggests facial recognition may "have the potential to exacerbate and entrench existing policing disparities along racial lines."

Cleaver's letter also took aim at Amazon — makers of facial recognition software, known as Rekognition, which is in use by some police agencies — saying that it was recently reported that the technology is "less accurate for African American subjects" and that Cleaver is "extremely concerned that facial recognition technologies will disproportionately burden African American communities."

According to The Hill (http://thehill.com/policy/technology/402147-dem-requests-doj-probe-on-law-enforcement-use-of-facial-recognition), Congressional Black Caucus Chairman Cedric Richmond (D-La.) sent a letter to Amazon in May, voicing concern about potential misuse of the technology.

Read more about Investigations (/tags?tag=Investigations) civil rights cases (/tags?tag=civil+rights+cases) Facial Recognition (/tags?tag=Facial+Recognition) Department of Justice (/tags?tag=Department+of+Justice) Artificial Intelligence (/tags?tag=Artificial+Intelligence) patrol (/tags?tag=patrol)

0 Comments

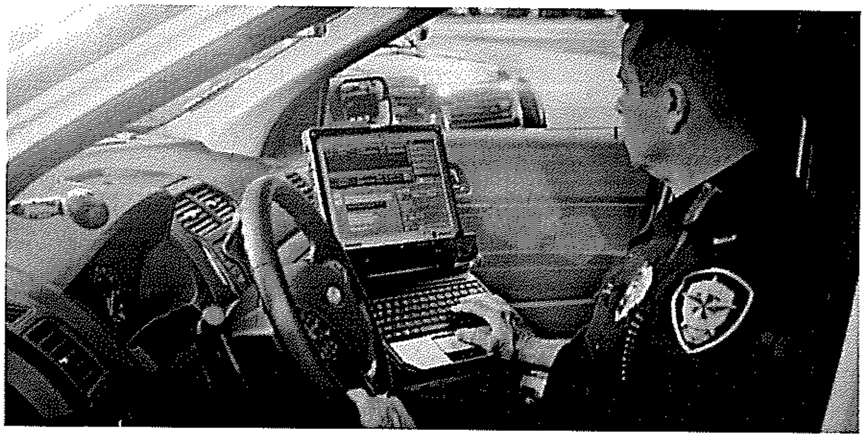
Join the discussion...

MORE

TECHNOLOGY

NEWS (/NEWS)

Panasonic to Take Part in Panel at IACP Technology Conference (/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)



(/513399/panasonic-to-take-part-in-panel-at-iacp-technology-conference)

The IACP Technology Conference is taking place in Jacksonville, FL, May 20–22. At the event on Tuesday, May 21, at 4 pm ET, Panasonic will take part in the panel discussion, "Managing Officer Safety Now and in the Future through a Strong Technology Ecosystem."

NEWS (/NEWS)

Video: Could a Robot Make Traffic Stops Safer? (/512502/video-could-a-robot-make-traffic-stops-safer)

(/512502/video-could-a-robot-make-traffic-stops-safer)

Once the officer's vehicle is parked behind the motorist's car, GoBetween rolls up to the driver's side window of the motorist, where it becomes the officer's eyes, ears and mouth. A spike strip automatically placed in front of the car's rear wheels keeps the motorist from driving away until the traffic stop is completed.

NEWS (/NEWS)

Knightscope Adds Facial Recognition to K1 Security Robots (/512416/knightscope-adds-facial-recognition-to-k1-security-robots)

"Prospective clients were able to upload a photo into the Knightscope Security Operations Center (KSOC) and then watch the K1 detect and report them as they moved about the booth. One creative individual even attempted to elude 'capture' by donning a pair of dark sunglasses to no avail," the company says.

NEWS (/NEWS)

Gamber-Johnson Wins WI Governor's Export Achievement Award (/512377/gamber-johnson-wins-wi-governors-export-achievement-award)

Gamber-Johnson has been named the recipient of the 2019 Governor's Export Achievement Award by the Wisconsin Economic Development Corporation (WEDC) for its contribution to Wisconsin's exporting strength.

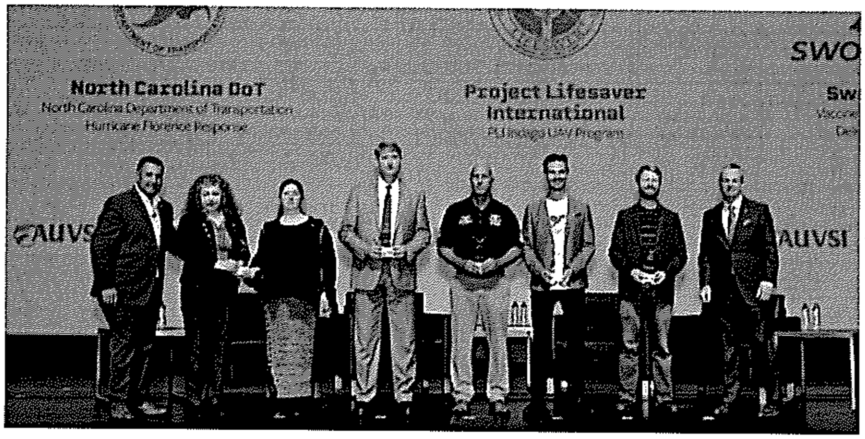
NEWS (/NEWS)

San Francisco Could Ban Use of Facial Recognition by Law Enforcement (/512178/san-francisco-could-ban-use-of-facial-recognition-by-law-enforcement)

The proposal, introduced by San Francisco Supervisor Aaron Peskin, would also require public input and the supervisors' approval before agencies buy investigative technology with public funds. That includes the purchase of license plate readers, toll readers, closed-circuit cameras, body cams, and biometrics technology and software for forecasting criminal activity.

NEWS (/NEWS)

Project Lifesaver International Receives Prestigious International Humanitarian Award (/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

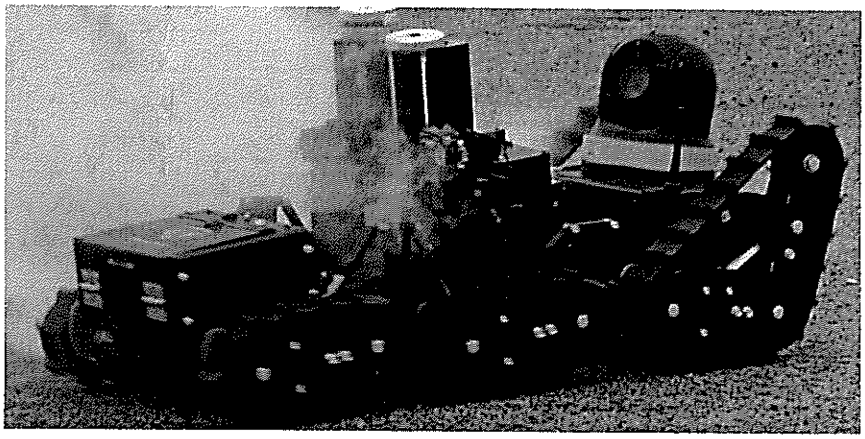


(/511812/project-lifesaver-international-receives-prestigious-international-humanitarian-award)

Project Lifesaver International (PLI) has been awarded the Humanitarian Xcellence Award by the Association for Unmanned Vehicles Systems International for its use of DJI drones to locate missing persons.

NEWS (/NEWS)

Transcend Tactical Introduces Mobile Gas Deployment System for Robots (/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)



(/511756/transcend-tactical-introduces-mobile-gas-deployment-system-for-robots)

Transcend Tactical has launched a gas deployment system that can be added to its Vantage robot to deploy two hot or cold gas grenades remotely and with mobility.

SPONSORED BY MOTOROLA SOLUTIONS

The Role of Data Analytics in Intelligence-Led Policing (/511412/the-role-of-data-analytics-in-intelligence-led-policing)

An agency's data is only as good as what it allows them to do next. Public safety agencies can increase situational awareness and decrease crime in the community by utilizing data analytics to the fullest extent.

NEWS (/NEWS)

NYPD Testing Virtual Reality-Based Training (/511543/nypd-testing-virtual-reality-based-training)

(/511543/nypd-testing-virtual-reality-based-training)

The NYPD is testing a virtual reality scenario-based training system. About 200 officers participated in the training program, which was conducted earlier this month at a state-of-the-art facility in Williamsburg, Brooklyn.

NEWS (/NEWS)

Axon Develops Tool for Measuring Officer Performance and Identifying Training Needs Through Body Camera Footage (/511538/axon-develops-tool-for-measuring-officer-performance-and-identifying-training-ne)

Axon has announced the launch of Axon Performance, a data analytics tool that helps to streamline the policy review process for law enforcement agencies. Axon Performance allows supervisors to more efficiently review video footage, perform agencywide officer performance evaluations, identify training needs and save officers time so they can spend more time in their communities.

LOAD MORE (/363041/LAWMAKER-ASKS-DOJ-TO-PROBE-POLICE-USE-OF-FACI/

Search (/search) | ☰ Menu

POLICE (/)
THE LAW ENFORCEMENT MAGAZINE

Search Menu

Training & Careers (/training-careers) Special Units (/special-units) Patrol (/patrol) Technology (/technology) Vehicle Ops (/vel

PATROL

Florida Department Extends Test of Amazon's Facial Recognition Software

July 9, 2018 • by Staff Writer (/authors/504428/staff)

Embed from Getty Images (http://www.gettyimages.com/detail/90339752)

The Orlando Police Department plans to continue its test of Amazon's controversial "Rekognition" facial recognition software, despite opposition (https://www.policemag.com/blog/technology/story/2018/06/balancing-privacy-rights-and-facial-recognition-technology-for-police.aspx) from civil rights groups such as the ACLU and even company employees and investors.

Rekognition can identify a person in a crowd matching an image uploaded to the system and track their movements in real time. The department had been using a free "proof of concept" trial of the system with seven police officers who volunteered to participate having images uploaded.

According to the Orlando Sentinel (http://www.orlandosentinel.com/news/orange/os-orlando-extends-amazon-test-20180709-story.html), the department informed Mayor Buddy Dyer and the city council that more time was needed to make a "thoughtful, precise and comprehensive recommendation" on whether or not the city should eventually purchase the technology.

Read more about technology (/tags?tag=technology) Facial Recognition (/tags?tag=Facial+Recognition) Florida (/tags?tag=Florida) the south (/tags?tag=the+south) ACLU (/tags?tag=ACLU) Florida agencies (/tags?tag=Florida+agencies) Biometrics (/tags?tag=Biometrics)

0 Comments

Join the discussion...

MORE

PATROL

NEWS (/NEWS)

Texas Police Officer Struck by Suspected Drunk Driver (/513407/texas-police-officer-struck-by-suspected-drunk-driver)

An officer with the San Marcos (TC) Police Department was severely injured when she was struck by a vehicle on Saturday night.

NEWS (/NEWS)

Detroit Police Officer Recovering After Being Shot (/513406/detroit-police-officer-recovering-after-being-shot)

An officer with the Detroit Police Department is recovering after being shot Saturday trying to stop a speeding driver on Saturday night.

NEWS (/NEWS)

Kentucky Officer Struck By Car While Investigating Vehicle Break-In (/513405/kentucky-officer-struck-by-car-while-investigating-vehicle-break-in)

An officer with the Louisville Metro Police Department was injured after being hit by a vehicle early Sunday morning.

NEWS (/NEWS)

Illinois Man in Custody Fires Gun Inside Police Department (/513404/illinois-man-in-custody-fires-gun-inside-police-department)

A man arrested for suspected theft and battery drew a gun inside the Carbondale (IL) Police Department and opened fire.

NEWS (/NEWS)

Georgia Officer Delivers Baby at Gas Station (/513403/georgia-officer-delivers-baby-at-gas-station)

An officer with the Hazlehurst (GA) Police Department was called to a local gas station to assist in the delivery of a baby boy late last week.

NEWS (/NEWS)

Proposed Massachusetts Bill Would Impose Death Penalty for Cop Killers (/513402/proposed-massachusetts-bill-would-impose-death-penalty-for-cop-killers)

According to Fox News, the proposed legislation would give judges the option of sentencing people over 18 to death for killing a police officer.

NEWS (/NEWS)

Connecticut Officer Saves Couple from Burning Home (/513401/connecticut-officer-saves-couple-from-burning-home)

An officer with the Shelton (CT) Police Department has been credited with saving the lives of a couple whose home suffered extensive damage from an early-morning fire.

NEWS (/NEWS)

Suspect in Killing of AL Officer Captured (/513346/suspect-in-killing-of-al-officer-captured)

Auburn police say the three officers were responding to a domestic disturbance call about 10 p.m. When they arrived on the scene they were reportedly fired upon by the suspect, identified as Wilkes.

NEWS (/NEWS)

AL Officer Killed—2 Wounded, Suspect at Large (/513338/al-officer-killed2-wounded-suspect-at-large)

The three officers were shot late Sunday night at a mobile home park in Auburn and a manhunt is underway for a suspect wearing body armor. One of the other two wounded officers is in critical condition. Both are expected to survive.

NEWS (/NEWS)

Tourniquet, Ballistic Vest Save Life of Oregon Officer After Being Shot (/513181/tourniquet-ballistic-vest-save-life-of-oregon-officer-after-being-shot)

(/513181/tourniquet-ballistic-vest-save-life-of-oregon-officer-after-being-shot)

An officer with the Salem (OR) Police Department is recovering after being shot several times during a traffic stop on Tuesday night.

LOAD MORE (/362344/FLORIDA-DEPARTMENT-EXTENDS-TEST-OF-AMAZONS-FA

(f (🐦 (in (⌘ (◎ (▶

Search (/search) | ☰ Menu