The New York State
Chief's Chronicle

Serving New York's Police Executives Since 1901 December 2018

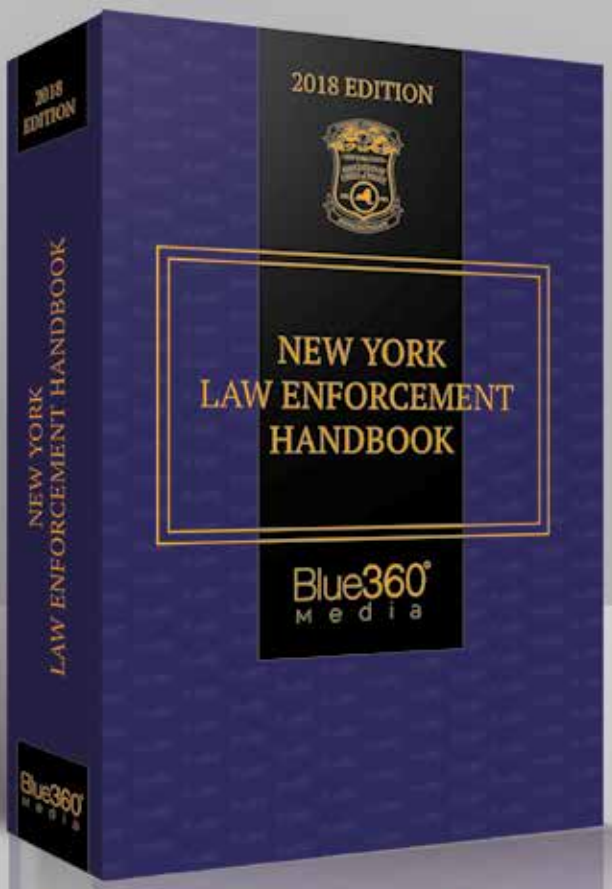
The New York State Department of Environmental Conservation and State Office of Fire Prevention and Control demonstrate how a drone can deliver a life vest to an individual stranded in rushing water. This demonstration was held in the new Swift Water/ Flood Rescue training facility at the State Preparedness Training Center in Oriskany. The New York State Division of Homeland Security and Emergency Services operates the State Preparedness Training Center.

Photo credit John Clifford, Rome Sentinel.

IN THIS EDITION:
Counsel's Corner
Feature Article - Harnessing the "Eye in the Sky" - An Overview of Drone Training
The New and Evolving Technology Challenges for Law Enforcement
Operation SafeCam
Finding Your Voice
The Allure of FirstNet

Blue360° Media

Blue360° Media is pleased to commemorate its partnership with the New York State Association of Chiefs of Police.



CO-PUBLISHED WITH NEW YORK STATE ASSOCIATION OF CHIEFS OF POLICE

- Complete and indespensable legal guide for New York law enforcement professionals.
- Includes Police Procedure: Laws of Arrest, Search and Seizure, and Confession Law.
- Features a special informational section — the "Blue Pages"-- from the New York State Association of Chiefs of Police.

WWW.BLUE360MEDIA.COM

2750 Rasmussen Road, Suite 107
Park City, Utah 84098
844-599-2887

contents

VOLUME 6 • ISSUE 4 • WINTER 2018

In this issue

2 **ON THE COVER**

3 **COUNSEL'S CORNER**
By Chief (Ret.) Michael D. Ranalli, Esq.

5 **LEADERSHIP: CONFIDENCE IN THE FACE OF CHALLENGES**

6 **INTELLIGENCE ADVISORY: HACKING POLICE CAMERAS**
Original article reprinted with the permission of the Northeast Ohio Regional Fusion Center

7 **HOW GANGS ARE USING DRONES TO DISRUPT LAW ENFORCEMENT**
By Robert Brzenchek, Alumnus, Intelligence Studies at American Military University

8 **THE NEW AND EVOLVING TECHNOLOGY CHALLENGES FOR LAW ENFORCEMENT**

9 **HARNESSING THE "EYE IN THE SKY" TO SUPPORT LAW ENFORCEMENT RESPONSE OPERATIONS: AN OVERVIEW OF DRONE TRAINING IN NEW YORK STATE**
By Meghan Dudley and Terry Hastings, NYS Division of Homeland Security and Emergency Services

11 **RANSOMWARE ON THE RISE FBI AND PARTNERS WORKING TO COMBAT THIS CYBER THREAT**

14 **OPERATION SAFECAM**
Author Caroline Wojtaszek, Niagara County DA

16 **FINDING YOUR VOICE**
By Chief Kevin Sylvester, Ossining Police Department

18 **THE ALLURE OF FIRSTNET**
By Chief James Suitor, Town of Niagara Police Department

20 **THE IACP 2018 CONFERENCE**
Photos courtesy of Greg Austin

A publication of the
New York State Association of Chiefs of Police, Inc.
24 Century Hill Drive Latham, New York 12110
Office: 518-355-3371

Do you have an interesting law enforcement story or an article you would like to submit, photographs of member activities or field scenes?
Contact the editor: Larry Eggert at leggert@nychiefs.org

On the Cover:

The New York State Department of Environmental Conservation and State Office of Fire Prevention and Control demonstrate how a drone can deliver a life vest to an individual stranded in rushing water. This demonstration was held in the new Swift Water/Flood Rescue training facility at the State Preparedness Training Center in Oriskany. The New York State Division of Homeland Security and Emergency Services operates the State Preparedness Training Center.

Photo credit John Clifford,
Rome Sentinel


The New York State
Chief's Chronicle

Serving New York's Police Executives Since 1901 December 2018

The New York State Department of Environmental Conservation and State Office of Fire Prevention and Control demonstrate how a drone can deliver a life vest to an individual stranded in rushing water. This demonstration was held in the new Swift Water/Flood Rescue training facility at the State Preparedness Training Center in Oriskany. The New York State Division of Homeland Security and Emergency Services operates the State Preparedness Training Center.

Photo credit John Clifford, Rome Sentinel.

IN THIS EDITION:
Counsel's Corner
Feature Article - Harnessing the "Eye in the Sky" - An Overview of Drone Training
The New and Evolving Technology Challenges for Law Enforcement
Operation SafeCam
Finding Your Voice
The Allure of FirstNet

Counsel's Corner

The Trouble with *DeBour:* The Complexity of the Law Pertaining to New York State Street Encounters

BY CHIEF (RET.) MICHAEL RANALLI, ESQ.

For over 40 years the law of police-citizen street encounters in New York State has been governed by the framework established by the New York Court of Appeals in *People v. DeBour*.[1] The case established four levels of encounter:

1. **Level 1: Request for Information.** The standard for this level is "an objective credible reason not necessarily indicative of criminality." No seizure is allowed, and any person contacted has the right to walk away.
2. **Level 2: Common Law Right to Inquire.** The standard for this level is "a founded suspicion criminal activity is afoot." Again, no seizure is allowed but officers can ask more pointed and invasive questions, such as whether a person possesses any weapons.[2] An officer must be at this level to ask a person for consent to search.
3. **Level 3: Stop and Frisk.** The standard for this level is "reasonable suspicion" a person is committing, has committed or is about to commit a crime. Once this level of suspicion is attained, an officer may seize a person and, depending upon the circumstances, frisk the person for weapons as well.
4. **Level 4: Arrest.** The standard for this level is "reasonable cause,"[3] which is essentially the same as the more commonly known terminology of probable cause.

This New York approach extends the protections of the Fourth Amendment to the United States constitution far more broadly than the federal courts. The federal courts have adopted three levels of street encounters: consensual or voluntary encounters, investigative stops and arrests. The federal approach applies the protections of the Fourth Amendment only when there is a seizure of a person. As a result, a voluntary or consensual encounter is not scrutinized to the same level as such encounters in New York. The biggest difference is that under federal law a request for consent does not need to be supported by any level of suspicion.

In the 40 years that *DeBour* has been law in New York, no other state or federal circuit court has decided to follow the same type of tiered analysis. In other words, we are the only state that extends Fourth Amendment protections to what would be mere consensual encounters in almost every other jurisdiction in the country.[4]

The problem with the application of the *DeBour* levels is there are no clear-cut guidelines for each level[5]. In many rapidly unfolding situations it is difficult for officers to know exactly where they are in this scheme. No bells and whistles go off when you pass from one level to another. Every case is different and one apparently minor fact can make all the difference. Further, courts have ruled inconsistently, so cases that appear similar lead to different results.

I have been a student of New York street encounters for almost 30 years. One of my biggest frustrations as an author and an instructor is to try to make sense out of inconsistencies. Some judges also struggle with the inconsistencies created by the *DeBour* tiered approach. The dissenting opinions in a recent case decided by the 4th Department Appellate Division, and affirmed by the New York Court of Appeals, will illustrate the problem.

People v. Gates

A New York State trooper stopped a vehicle for speeding after 10:00 pm on a highway. The trooper noticed the rear of the vehicle sagged as if something heavy was in the back of the car or trunk. There were three male occupants of the vehicle and the officer noticed several large nylon bags on the back floor and seat. The bags protruded out with sharp edges indicating some type of hard objects were inside them. The trooper asked the driver where he was going, and he responded that he had been visiting family in Ohio. The occupants all appeared nervous and were avoiding eye contact with the trooper, who then asked if the bags contained luggage. The driver responded it was clothing, which was followed by a series of implausible answers. Finally, the driver admitted the bags contained close to 300 cartons of untaxed cigarettes. He was arrested.[6]

The County Court refused to suppress the evidence and the defendant appealed. The majority of the Appellate Division reversed, holding that the trooper's inquiry about the content of the bags was a Level 2 common-law inquiry, which was not supported by the required Level 2 "founded suspicion" of criminal activity. The Court stated, "Indeed, we note that nervousness, fidgeting, and illogical or contradictory responses to Level 1 inquiries do not permit an officer to escalate an encounter to a Level 2 *DeBour* Confrontation."[7] The Court cited two cases to support this broad statement, *People v. Garcia*[8] and *People v. Dealmeida*.[9]

There are two things wrong with this statement by the court. First, such a sweeping statement was not necessary under these facts. Right, wrong or otherwise, the Court ruled that asking about the content of the bags was an unsupported Level 2 inquiry. The driver's inconsistent statements did not come until *after* the inquiry about the contents, which the court acknowledges later in its decision. The court did not even need to address the impact of the driver's inconsistent answers. Instead, they make a statement that, to many readers, sounds like an established rule but instead is inappropriate dicta.

Which leads to the second problem: The cases cited do not support the Court's statements. In *Garcia*, the officer asked if the occupants of a vehicle had a weapon because they were acting nervous and made "furtive" movements. That was it—no illogical or contradictory statements. Citing that overly broad statement to *Garcia* is misleading. And in *Dealmeida*, the defendant was nervous and did give nonsensical answers to an inquiry about where he was coming from and going. He was then asked if he had anything illegal on him, which the court found was a Level 2 question (correct under *Garcia*), but that inquiry was not supported by the facts. But this case appears incorrectly decided because of the *Dealmeida* court's own explanation: "Defendant's nervousness and discrepancies in describing where he was coming from and going are not enough to give rise to a *reasonable suspicion* that criminal activity is afoot."[10] Who said anything about asking if someone has something illegal on them requiring *reasonable suspicion*—the standard for a Level 3 encounter?

If the courts that decide the appropriateness of police actions under *DeBour* do not understand it, how are police officers expected to follow it?

Two judges of the Appellate Division in *Gates* dissented, reasoning that in response to the defendant indicating he was coming back from Ohio, asking if his luggage was in the nylon bags was an additional Level 1 question. Further, his answer that the bags contained clothing led to yet an additional appropriate Level 1 inquiry about whether the clothing was in boxes because of the outline of the bags. That led to the conflicting answers, giving the trooper founded suspicion to support a further Level 2 inquiry.

So far, we have an even split among the judges who have ruled on this case. The County Court judge and the two dissenting judges felt the trooper acted appropriately. Three judges of the Appellate Division disagreed, resulting in an even split. Although judges cannot agree on what is appropriate, officers are supposed to know how to act within the *DeBour* confines on the street. All agree it is an appropriate Level 1 question to ask someone where they are coming from and going. If the person chooses to answer, which they do not necessarily have to do, then would it not make sense to use inconsistent or illogical answers as a basis for Level 2? If not, why allow the questions in the first place?

On appeal to the Court of Appeals, the majority merely ruled there was record evidence to support the Appellate Division determination with no evaluation of the case. Judge Garcia, however, disagreed with the majority and chose to write a dissenting opinion that questioned the viability of *DeBour*, especially in the context of traffic stops, which he believes are inherently more dangerous than other street encounters.

After reviewing the difficulties of distinguishing between Level 1 and Level 2, Judge Garcia stated, "Evidently, the *DeBour* sliding scale generates 'such confusion and uncertainty that neither police nor courts can ascertain with any degree of confidence precisely what it takes to meet any of these standards' (4 LaFave, Search and Seizure § 9.4[e]). The 'hyperstringent' rule of *DeBour* also serves as a barrier to legitimate, effective, and minimally-intrusive law enforcement practices designed to detect and ward off threats at their earliest states."[11]

The judge reviewed several inconsistencies in the law of street encounters. For example, officers can order occupants out of a vehicle on a traffic stop with no suspicion, but they cannot ask them if they have weapons without founded suspicion. Judge Garcia does a nice overview of the issues with *DeBour* and the decision is worth a read. A report issued by the New York State Bar Association Criminal Justice Section's Committee on Prosecution also concluded, "We have succeeded in creating an uneven enforcement of our laws, often not determined by the nature and quality of the evidence of guilt or innocence, but, rather, by the freakish quirks of fate visited by the application of a standard that does not mean the same thing to any two individuals, who participate in the criminal justice system. It is difficult not to conclude that, in the main, we would all be better without it."[12]

Dealing with *DeBour*

While we are left having to deal with the complexities of *DeBour*, the good news is that arguments against its viability are being raised and written. Perhaps the criticism will continue. But in the meantime law enforcement in New York must continue to function under the *DeBour* levels.

Having a proper mindset is important; officers must be prepared to act without being crippled by the complexity of the law. In my classes, I discuss the importance of working the "Gray Area." Imagine a chart with a red line to the left and a green line some distance away to the right. In between, from left to right, the chart goes from white through continuously darkening shades of gray until dark gray meets the green line. The red line stands for an improper or illegal action by an officer. The green line signifies an action that would be clearly legal so no court would disagree. We know that we cannot just walk up to someone and frisk them with no suspicion at all. That would be a red line action. If, however, we legally approached a person and saw a gun clearly visible in their waistband, a frisk would be a green line action.

Your officers have the ability to stay away from the red. There are clear and obvious actions that would be at or near the white and red and should be avoided. On the other end of the spectrum, however, is the reality that policing is rarely clear cut, especially when you must navigate standards applicable to the four *DeBour* levels. The goal of a police officer should be to get as far into the gray as possible, testify truthfully and thoroughly and hope it is enough.

This is the reality of the confusing and complicated analysis that develops from the law pertaining to street encounters in New York. As police administrators you must understand the difficulties your officers face and accept that you may lose some cases in court as a result. As long as your officers are trying to work within the law, they should be encouraged to shake off the losses and get back out there and try again.

(Endnotes)

[1]40 N.Y.2d 210 (1976)
[2]*People v. Garcia*, 20 N.Y.3d 317 (2012)
[3]NY Crim Proc Law § 70.10(2)
[4]NY State Bar Association, A Report of the Criminal Justice Section's Committee on Prosecution: *Close Encounters of the Police Citizen Kind: A National Study of Police Citizen Encounters in Other States and Federal Courts in Relation to PEOPLE v. DEBOUR (2018)*
[5]Note: This article contains some content from the upcoming 3rd Edition of my book *Search & Seizure Law of New York State: Street Encounters 3rd Edition*, published by Looseleaf Law Publications, Inc. The content used is new to the book for this edition and will be published in fall 2018.
[6]*People v. Gates*, 152 A.D.3d 1222 (4th Dept. 2017), *aff'd* 31 N.Y.3d 1028 (2018) (facts taken primarily from dissenting opinions)
[7]*Id*, at 1223 emphasis added
[8]20 N.Y.3d 317 (2012)
[9]124 A.D.3d 1405 (4th Dept. 2015)
[10]*Id.* at 1407, emphasis added
[11]People v. Gates, 31 N.Y.3d 1028, 1031)
[12]NY State Bar Association report, supra at 153. Note: This is the opinion of the authors of the report and the section committee and has not to my knowledge been adopted by the Bar Association.

Leadership

Confidence in the Face of Challenges

We sometimes may doubt our ability to accomplish a goal or task. Perhaps as early as grade school, we wanted to try out for a sports team or school play, but felt intimidated by the risk of failure. Questions swirled through our head. *What if I fail? What will my friends think?*

Today, we face "adult" challenges and potential consequences both personally and professionally. Those same haunting questions and thoughts of inadequacy may return to our minds, causing us to avoid confronting a trial or taking a risk. Pursuing a promotion, trying a different job-related task, or beginning a new relationship may seem intimidating. Do we miss out on personal or professional fulfillment because of our fear of failure?

Of course, we may question our abilities as a heathy recognition of our own limits. However, feelings of inadequacy alone never should serve as a license to quit or an excuse not to try. They often stem from false beliefs about ourselves or an exaggerated view of the challenge itself.

Could it actually hold true that you have the strength to climb the mountain? Is the peak not nearly as high as it looks from your vantage point? Allow yourself to rise to the occasion, accept the challenge, and realize your potential.

Some simple suggestions can help you gain the needed confidence to face a given situation.

1. *Identify the specific issue*. A job promotion seemingly may present an insurmountable hurdle. However, upon closer inspection, the promotional process—not the new job itself—could be the intimidating factor.
2. *Divide the challenge into manageable milestones*. As the old saying goes, "When eating an elephant, take one bite at a time."[1] This applies to many areas of life. For instance, getting physically fit may seem daunting. Set reasonable goals to improve incrementally. The small victories along the way will encourage you.
3. *Set a schedule and prioritize accordingly*. Does a huge project look impossible? Set definitive dates to reach objectives. Do not postpone completion dates because of things you can control.
4. *Leverage your strengths*. Alternative ways to accomplish a goal may exist. For example, a recent NFL draftee wanted to play in the league, but felt he did not have the speed or strength. His previous success as a soccer player led him to focus on his kicking ability. He achieved his ambition through this alternative route.

How far can you go in your career? What would you like to accomplish? You will never realize your full potential by fearing failure more than striving for success. Take a chance—you may surprise yourself.

Reprinted with the permission of the FBI Law Enforcement Bulletin. Supervisory Special Agent Donald L. Bostic of the Executive Programs Instruction Unit at the FBI Academy prepared this article. He can be reached at dlbostic@fbi.gov.

Intelligence Advisory: Hacking Police Body Cameras

(U) Executive Summary

(U) The Northeast Ohio Regional Fusion Center (NEORFC) prepared the following bulletin to address the potential for police body cameras to be hacked into, tracked, manipulated, or have malware installed on them. This bulletin is being provided for situational awareness to law enforcement and private sector partners on the cybersecurity concerns that may arise with the use of body cameras.

(U) Background

(U) Body cameras are often used as evidence in judicial proceedings, but are also worn to promote trust between police and the public by creating a greater sense of transparency and accountability

(U) DEF CON, one of the world's largest hacking conventions, was hosted in Las Vegas, Nevada from August 9th-12th 2018.[1] At the convention, Josh Mitchell, a consultant for security firm Nuix, demonstrated how body cameras are vulnerable to being hacked and provided several key findings.

(U) Mitchell tested cameras from five companies that market their devices to law enforcement agencies in the United States, including Vievu, Patrol Eyes, Fire Cam, Digital Ally and CeeSc.[2]

(U) In all but the Digital Ally device, video from the cameras could be downloaded, edited/modified or deleted, and then re-uploaded with no indication of the change.

U) Four out of five of the cameras, excluding CeeSc WV-8, operated on Wi-Fi radio, which broadcast identifying information about the device that could give away information like make, model, and device codes. This could be utilized to track police officers using a long-range antenna.[4]

(U) Body cameras are often activated when police carry out certain operations, such as raids, which may allow someone to recognize when numerous body cameras are activated in one localized area that an operation is about to occur.[5]

(U) Outlook

(U) Findings from Mitchell's study have been shared with the body camera companies he tested, and Mitchell is currently working with some of them to address the security issues.[6]

(U) There is an additional concern with the potential for video recordings of victims of domestic violence, sexual assault or child abuse to be accessed and modified.[7]

(U) Police body cameras can also be compromised with malware which would be downloaded to the computer that is linked to the body camera, and potentially spread to infiltrate the department's servers and police network.[8]

(U) Many police departments rely on default credentials that are set up with the cameras, but even departments who have been proactive in updating the default settings are still at risk.[9]

(U) The NEORFC has not received any reporting of malicious cyber intrusion into police body cameras in Northeast Ohio.

Original article reprinted with the permission of the Northeast Ohio Regional Fusion Center

How Gangs are Using Drones to Disrupt Law Enforcement

BY ROBERT BRZENCHEK, ALUMNUS, INTELLIGENCE STUDIES AT AMERICAN MILITARY UNIVERSITY

Gangs are continually adapting their skillsets to counter law enforcement efforts. For example, as outlined in my book, "The Gang Life Laugh Now Cry Later: Suppression and Prevention," gangs have sent their members into the military to gain tactical skillsets. In other cases, gangs have coordinated with terrorist organizations and are acting as "sub-contractors" to groups like ISIS and Al-Qaeda.

As gangs are finding new and better ways to disrupt community safety, they are getting alarmingly proficient at using unmanned aerial vehicles (UAVs) – also commonly referred to as drones – to support their criminal activity.

Organized criminal elements will continue to find creative and effective ways to use UAV technology for illegal activity.

HOW GANGS ARE USING DRONES

Gangs are now using UAVs to monitor and disrupt police. As reported by *The Washington Times*, FBI Special Agent Joe Mazel described how criminal gangs recently compromised officers who were part of a Hostage Rescue Team. "[Agents] heard the buzz of small drones – and then the tiny aircraft were all around them, swooping past in a series of high-speed low passes at the agents in the observation post to flush them," he said.

Gangs are also using UAVs to collect information about police activity. For example, they are using drones to watch law enforcement agencies to see who comes in and out of buildings. They are then using this information to intimidate witnesses who are cooperating with police investigations.

It has also been reported by Fox News numerous times that gangs and drug cartels are using large UAVs to smuggle drugs across the border. Even more dangerously, they have been placing explosives on the exterior of the UAVs so if law enforcement interdicts these devices, officers can potentially be harmed. Officers must be extremely cautious when responding to an incident involved a UAV since there could be multiple threats associated with the device.

HOW GANGS ARE COMPROMISING POLICE DRONES

In addition, gangs have reportedly found ways to hack certain brands of drones used by police. It was reported by CNBC that at least one UAV manufacturer, Dà-Ji ng Innovations (DJI), a Chinese technology company, is vulnerable to hacking. According to sUAS news, the DJI is an open-source system controlled by a cell phone and is vulnerable to hackers to collect data and assume control, too.

While the Department of Defense has blacklisted DJI drones, some police departments have purchased the devices either because they're unaware of the restriction or because of the low cost of the devices. According to *The New York Times*, a United States government office is alleging these devices pose a threat to national security because DJIs metadata may be sending sensitive information about American infrastructure back to China.

Hacking or taking control of unencrypted UAVs is something that gangs are interested in doing as well. In order to do so, gangs have recruited members who are IT specialists. These technology-savvy individuals have figured out, for example, how to geo-fence properties where criminal activities occur. If a police agency using an unencrypted UAV (i.e. DJI) is conducting surveillance and enters this area, the geo-fence disrupts communication to the drone entering that area. The drone is unable to send and receive information and the geo-fence takes over controls to and from operators on the ground, forcing the UAV to crash.

Hackers are able to collect data/control a law enforcement drone by utilizing a type of malware such as Maldrone. Another way hackers can gain access to a drone is through another drone (i.e., SkyJack) that mid-flight hacks into a law enforcement drone via internet connections. The gang can then retrieve the SD memory card from the DJI drone and potentially access all the intelligence collected from the device.

UPDATING LEGISLATION TO ADDRESS CRIMINAL USE OF DRONES

Organized criminal elements will continue to find creative and effective ways to use UAV technology for illegal activity. They will continue doing so unless law enforcement works closer with policymakers to enact uniform laws, regulations, and policies beyond the FAA Part 107. Lawmakers must work harder to address issues related to drone operation and enact laws that help agencies address the challenges they face when it comes to drone enforcement and operation.

In addition, regulations need to be created to protect agencies and mandate they only purchase encrypted UAVs, so if the devices fall into the wrong hands, the information stored within them can't be collected and used for illicit purposes.

This article was re-printed with the permission of the American Military University and originally published on American Military University's site, InPublicSafety.com

About the Author: *Robert M. Brzenchek is the Chief Executive Officer of All Source International, LLC, a security consultancy company based in Philadelphia. He earned a master's degree in intelligence studies from American Military University and is currently a Ph.D. candidate at Capella University with a proposed dissertation focused on gangs. To contact him, email IPSauthor@apus.edu. For more articles featuring insight from industry experts, subscribe to In Public Safety's bi-monthly newsletter.*

The Erie County Public Safety Campus on Elm Street in Buffalo, NY, where the Western New York Regional Computer Forensic Laboratory (WNY RCFL) is housed.

The New and Evolving Technology Challenges for Law Enforcement

Law Enforcement encounters digital evidence in almost every investigation—awareness, training and communication are keys to recovering it.

In the ever-growing cyber world, law enforcement's use of digital forensics is critical in locating and retrieving stored evidence previously hidden from the eyes of an investigator. For law enforcement, the challenge to collect this evidence is lessened when investigators are familiar with the wide variety of items designed to hold information. Today, digital evidence is routinely recovered from USB drives, SD cards, watches, fitness trackers, tablets, gaming systems, laptops, desktops, and even motor vehicles. Training in the recognition and proper collection of items containing digital evidence is a priority.

To help combat this relatively-new and evolving challenge for law enforcement, The FBI's Regional Computer Forensics Laboratories (RCFLs) located across the country are one-stop, full-service forensic labs and training centers where highly-trained forensic examiners process a wide array of digital evidence.

In law enforcement, we know that a critical key to investigative success is communication. Talking to other law enforcement officials who have had success in exploiting digital evidence, sharing best practices, and reaching out for support when an agency encounters a roadblock, are all important steps when facing the challenges of digital evidence preservation and collection.

> We leave a digital trail behind as we all go about our daily lives.

Smartphones remain a significant source of digital evidence; however, access controls utilized on these devices can prove an obstacle for investigators. The RCFL has a message to investigators: Don't give up if you're having difficulty recovering smartphone evidence. Instead, reach out to your local FBI RCFL or computer forensic laboratory to ask about newer tools available to assist you. As technology continues to evolve so do the tools available for investigators to use.

While smartphones hold a cache of potential digital evidence, there are other items likely to contain valuable information. Watches often have embedded location programs that sync with a computer and smartphone. The RCFL in Buffalo assisted with a local homicide investigation where the subject did not have his smartphone with him when he committed the crime, but he was wearing a smartwatch. The suspect's watch eventually synced with his smartphone and investigators used the resulting timeline to obtain an indictment. While relying on cell tower information to gather evidence can leave gaps in an investigation, pulling information from digital devices can reduce or eliminate those gaps.

FBI Supervisory Special Agent/RCFL Director Matthew Giacobbi (pictured standing), Niagara County Sheriff's Office Task Force Officer Christopher Page (pictured foreground) confer about information displayed on a Cellebrite machine.

We leave a digital trail behind as we all go about our daily lives. Consider video surveillance, for instance. There was a time when video surveillance was primarily used for security in banks and commercial businesses, and the quality of the dated equipment left us with grainy images. Advancements in technology has allowed

—TECHNOLOGY CHALLENGES, continued on Page 13

Harnessing the "Eye in the Sky" to Support Law Enforcement Response Operations: An Overview of Drone Training in New York State

BY MEGHAN DUDLEY AND TERRY HASTINGS,
NYS DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

Drone Training at SPTC

Unmanned Aircraft Systems (UAS) provide a new and exciting tool for law enforcement agencies and other first responder organizations to safely, effectively, and efficiently enhance their capabilities in many different functional areas. Law enforcement agencies in New York State are already using UAS for a multitude of operations, including situational awareness during major incidents, for complex bomb squad and tactical team operations, and to enhance and streamline reconstruction efforts after traffic accidents.

While the use of UAS in the law enforcement arena provides many benefits, it comes with significant challenges as well. The Federal Aviation Administration (FAA) governs the use of small UAS (those weighing from .55 lbs. to 55 lbs.) in the United States.

> Based on the feedback from the Focus Group (and other related outreach efforts), DHSES developed a series of new and innovative UAS courses at the SPTC.

The governance framework put forth by the FAA has changed significantly over the past several years and is often not well understood within the first responder community. Additionally, the use of UAS by law enforcement agencies can be controversial in some communities, as there have been public concerns regarding the use of drones.

Given the proven benefits and potential challenges involved in the use of UAS, the New York State Division of Homeland Security and Emergency Services (DHSES) recognized that it could provide leadership, coordination, and training to assist law enforcement and other first responder agencies in the development of their UAS programs. First, DHSES created a "UAS Working Group" comprised of numerous State Agencies, including the New York State Police (NYSP), Department of Environmental Conservation (DEC), Metropolitan Transportation Authority (MTA) and others, to understand current capabilities, challenges, technology, and best practices. Next, DHSES hosted a "UAS Training Focus Group" in July 2017 at the State Preparedness Training Center (SPTC) in Oriskany. The UAS Focus Group brought together more than 70 local, state, and Federal representatives to discuss the use of drones in the public safety realm and to identify training needs and priorities.

Based on the feedback from the Focus Group (and other related outreach efforts), DHSES developed a series of new and innovative UAS courses at the SPTC.

DHSES Commissioner Roger L. Parrino, Sr. stated, *"Drones provide an exciting new opportunity for public safety organizations to enhance their capabilities, while also reducing risks to first responders who can be kept out of harm's way by using the technology. DHSES has developed a series of innovative, comprehensive UAS programs for first responders statewide, in conjunction with our partner agencies. The State Preparedness Training Center in Oriskany provides a world-class venue for this training and it aligns with Governor Cuomo's initiative to build a "drone corridor" in the Mohawk Valley."*

The Center's current UAS trainings include:

- **UAS Awareness Workshop:** This one-day workshop, developed in partnership with DEC, provides agencies with essential information as they begin a UAS program, including FAA doctrine and the Part 107 process (which is the FAA's certification exam for UAS pilots), UAS challenges and best practices, and counter-UAS considerations.
- **UAS Part 107 Preparation Course:** This two-day course is designed to help law enforcement officers and other first responders to prepare to take their FAA Part 107 Exam. This is the SPTC's newest UAS course (piloted in October 2018) and it was developed in partnership with DEC.
- **UAS Basic Operator Course:** DHSES, in conjunction with UAlbany's National Center for Security and Preparedness (NCSP), developed a five-day Basic Operator School. The Albany County Sheriff's Office and DEC provided critical support to DHSES and the NCSP in the development of this course, which was piloted in late 2017. This course covers legal and ethical UAS operations, flight authorizations, crew resource management, pre-flight decision making, risk analysis, mission planning, record keeping, photography and video, and practical flight exercises and scenarios.
- **UAS Advanced Operator Course:** In partnership with NCSP, DHSES developed a two-day Advanced Operator Course that was piloted in September of 2018. This course involves In-Flight Emergency Operations (including loss of application, loss of visual line-of-sight, see and avoid, and manually determining aircraft orientation); scenario based activities, and an optional night flight component.

DHSES also sponsored the first Public Safety UAS Summit at the SPTC in August of 2018. This event brought together over 100 stakeholders from across New York State (and the country) to hear ▶

Mavic Pro

Fortem
Drone Hunter

Black Hornet

Drone Training at SPTC

Phantom 4

MQ9 Reaper

Photos Courtesy of Chief Mark Pacholec, Orchard Park PD

from national UAS experts on current and emerging issues and technological advancements.

DHSES relied heavily on State and local law enforcement agencies to develop these training programs. Lieutenant Frank Carbone, from the New York State Department of Environmental Conservation Police, said "The DEC is proud to support DHSES in the development and delivery of UAS training programs at the SPTC. The DEC has a mature UAS program and our best practices

> To date, more than 300 first responders have received UAS training at the SPTC.

and lessons learned are a resource for other first responder agencies to utilize as they begin their own UAS efforts."

The NYSP have also been a major partner to DHSES's UAS training efforts. Captain Scott Reichel, from the NYSP Field Command said, "*DHSES UAS training has been extremely helpful to the New York State Police as we continue to develop our UAS capability. UAS training by DHSES provides a resource that some departments might not otherwise be able to obtain, while simultaneously providing a common operating standard for law enforcement across New York state to operate UAS effectively and in accordance with FAA regulations.*"

To date, more than 300 first responders have received UAS training at the SPTC. DHSES will continue to build and adapt its courses to meet the current needs of law enforcement and the first responder community in New York State, thus harnessing the "Eye in the Sky" to support the effective, ethical, and safe use of UAS technology to support public safety missions.

For more information on UAS (and other) training programs at the SPTC, visit:
http://www.dhses.ny.gov//training/calendar/?agency=SPTC

Meghan Dudley is an Intelligence Analyst with DHSES and oversees Training Administration at the State Preparedness Training Center (SPTC). Terry Hastings serves as the Senior Policy Advisor for the NYS Division of Homeland Security and Emergency Services (DHSES).

Ransomware on the Rise

FBI and Partners Working to Combat This Cyber Threat

Your computer screen freezes with a pop-up message—supposedly from the FBI or another federal agency—saying that because you violated some sort of federal law your computer will remain locked until you pay a fine. Or you get a pop-up message telling you that your personal files have been encrypted and you must pay to get the key needed decrypt them.

> Ransomware has been around for several years, but there's been a definite uptick lately in its use by cyber criminals.

These scenarios are examples of ransomware scams, which involve a type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom—anywhere from hundreds to thousands of dollars—is paid.

Ransomware doesn't just impact home computers. Businesses, financial institutions, government agencies, academic institutions, and other organizations can and have become infected with it as well, resulting in the loss of sensitive or proprietary information, a disruption to regular operations, financial losses incurred to restore systems and files, and/or potential harm to an organization's reputation.

> Also, a growing problem is ransomware that locks down mobile phones and demands payments to unlock them.

Ransomware has been around for several years, but there's been a definite uptick lately in its use by cyber criminals. And the FBI, along with public and private sector partners, is targeting these offenders and their scams.

When ransomware first hit the scene, computers predominately became infected with it when users opened e-mail attachments that contained the malware. But more recently, we're seeing an increasing number of incidents involving so-called "drive-by" ransomware, where users can infect their computers simply by clicking on a compromised website, often lured there by a deceptive e-mail or pop-up window.

Another new trend involves the ransom payment method. While some of the earlier ransomware scams involved having victims pay "ransom" with pre-paid cards, victims are now increasingly asked to pay with Bitcoin, a decentralized virtual currency network that attracts criminals because of the anonymity the system offers.

Also, a growing problem is ransomware that locks down mobile phones and demands payments to unlock them.

The FBI and our federal, international, and private sector partners have taken proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets that facilitated the distribution and operation of ransomware. For example:

- Reveton ransomware, delivered by malware known as Citadel, falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites or other illegal online activity. In June 2013, Microsoft, the FBI, and our financial partners disrupted a massive criminal botnet built on the Citadel malware, putting the brakes on Reveton's distribution. FBI statement and additional details.
- Cryptolocker was a highly sophisticated ransomware that used cryptographic key pairs to encrypt the computer files of its victims and demanded ransom for the encryption key. In June 2014, the FBI announced—in conjunction with the Gameover Zeus botnet disruption—that U.S. and foreign law enforcement officials had seized Cryptolocker command and control servers. The investigation into the criminals behind Cryptolocker continues, but the malware is unable to encrypt any additional computers. Additional details.

If you think you've been a victim of Cryptolocker, visit the Department of Homeland Security's U.S. Computer Emergency Readiness Team (CERT) CryptoLocker webpage for remediation information.

The FBI—along with its federal, international, and private sector partners—will continue to combat ransomware and other cyber threats. If you believe you've been the victim of a ransomware scheme or other cyber fraud activity, please report it to the Bureau's Internet Crime Complaint Center.

LATEST RANSOMWARE THREAT

A fairly new ransomware variant has been making the rounds lately. Called CryptoWall (and CryptoWall 2.0, its newer version), this virus encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It directs the

user to a personalized victim ransom page that contains the initial ransom amount (anywhere from $200 to $5,000), detailed instructions about how to purchase Bitcoins, and typically a countdown clock to notify victims how much time they have before the ransom doubles. Victims are infected with CryptoWall by clicking on links in malicious e-mails that appear to be from legitimate businesses and through compromised advertisements on popular websites. According to the U.S. CERT, these infections can be devastating and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

PROTECT YOUR COMPUTER FROM RANSOMWARE

- Make sure you have updated antivirus software on your computer.
- Enable automated patches for your operating system and web browser.
- Have strong passwords, and don't use the same passwords for everything.
- Use a pop-up blocker.
- Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars).
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.
- To prevent the loss of essential files due to a ransomware infection, it's recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline.

Editors note: A few years ago, while Chief of Police in Lockport, our department was the victim of a ransomware attack. At the time there was no effective method to reverse the attack. The only options at the time were to pay the ransom or wipe our computers clean of all data and begin from scratch. It is imperative that police departments take measures to protect their records infrastructure to prevent a successful attack.

See also: *https://www.healthdatamanagement.com/news/erie-county-medical-center-anatomy-of-a-ransomware-attack*

Reprinted from
https://www.fbi.gov/news/stories/ransomware-on-the-rise. January 2015

—TECHNOLOGY CHALLENGES, continued from Page 8

for the marketing of affordable high-definition video cameras and recorders. Video surveillance systems are increasingly popular with small businesses and homeowners. Whether through a doorbell camera, a wireless system recording to the cloud, or a wired system connected to a DVR, the capturing of criminal activity on personal video equipment has increased. Cameras are now instrumental in solving a wide-range of crimes, from larcenies to hit and runs to arsons.

> Another technical advancement in digital evidence collection involves motor vehicles.

It is critical to collect video evidence properly once a camera is located. Law enforcement must work with equipment owners to obtain images quickly, as each system has different recording capabilities. Acting quickly is crucial to limit the possibility that valuable video evidence is recorded over. With so many different proprietary video systems on the market, contacting a local RCFL examiner or someone trained in retrieving digital evidence before removing or unplugging surveillance systems is imperative. At the RCFL in Buffalo, we have encountered instances where investigators delivered DVRs for examination, but due to age of the system and the proprietary nature of the software, when examiners attempted to power up the devices to retrieve data the drives reformatted. In these cases, better communication or a phone call prior to bagging and tagging the evidence was necessary.

Another technical advancement in digital evidence collection involves motor vehicles. Historically, investigators pulled GPS systems and black boxes to retrace the route of a vehicle or to obtain valuable information. Today, with automobiles continuing to become more technologically advanced and reliant on computers, investigators could potentially have additional evidence at their disposal which historically has not been possible.

> Communication and training are important to achieve success in a digital evidence investigation.

Forensic tools can often be used to yield detailed vehicle activity reports to include odometer readings, system information, gearshift activity, door activity, hard accelerations and hard braking, wheel traction, and navigation. An examination can also provide information from phones and USB drives previously connected to the vehicle.

It is important to remember that subjects may also attempt to obscure digital information. Many devices allow owners to remotely wipe information. With training, investigators can do more to protect potential evidence. For example, seizing investigators should immediately put cellphones in airplane mode to prevent smartphones from receiving and sending radio frequency signals, thereby protecting the contents from possible remote erasure.

Display case holding historical digital evidence, including several unique thumb drives (top shelf), located in the entryway to the WNY RCFL.

And remember to rely on good interviewing skills to secure passwords and passcodes. Since there is a need to keep track of so many passwords and passcodes today, most people resort to documenting them somewhere.

Communication and training are important to achieve success in a digital evidence investigation. Sharing information with your peers is crucial. Investigators should communicate with outside law enforcement partners to stay current on evolving technology and available training opportunities, with the goal to increase success in the world of digital evidence collection.

Develop best practices in your department. And, when you stumble into unforeseen roadblocks, reach out to your local RCFL to see if examiners can assist you in collecting digital evidence. In law enforcement we need to continuously train and advance to maintain the high standards expected by the public we serve.

Operation SafeCam

In August of 2017, the Niagara County District Attorney Caroline Wojtaszek announced the implementation of Operation SafeCam throughout Niagara County, New York. Operation SafeCam was born of the need to have more intelligence available to our police when crime occurs. It is a public safety program that provides police access to private security cameras to assist in solving crimes. The cameras provide coverage when police are not in the right place

> The SafeCam program empowers the public to help law enforcement in fighting crime in our community by expanding the county's surveillance camera database.

and time to apprehend a criminal. This program was modeled after a similar program developed by Buffalo, New York Police Commissioner Daniel Derenda and Mayor Byron Brown and was initially developed by the Philadelphia Police Department.

Niagara County has three cities including the City of Niagara Falls. We share a border with Canada and is home to three major border crossings into Canada. The County also has 12 towns and several villages and hamlets, each with their own unique law enforcement challenges. Crime patterns vary widely depending on location, season and time of day. Our county also attracts a very large tourist population at various times of the year because of its geographical proximity to Canada. These logistical challenges create many challenges for law enforcement when addressing criminal activity.

HOW DOES OPERATION SAFECAM WORK

The SafeCam program empowers the public to help law enforcement in fighting crime in our community by expanding the county's surveillance camera database. The goal of the program is to work with the community to help blanket the county with security cameras that will assist in criminal investigations. This goal is accomplished by identifying city/county businesses as well as private residents that have privately owned cameras mounted on their property. These business owners and residents are then asked to register their cameras with their local police department. One can register by simply filling out a form found on the District Attorney Office's website. Through Operation SafeCam, local law enforcement will have previous knowledge of where cameras are located throughout their individual jurisdictions. This knowledge will save time, on the front-end of their investigations, allow quick access to any video evidence, and increase the solvability factors essential to quickly arresting the perpetrators and solving the crime.

To help increase the camera inventory across the county, the District Attorney's Office utilized $60,000 from our Asset Forfeiture Funding to provide six fixed cameras and one mobile license plate reader. In April 2018, in coordination with the City of Niagara Falls, four additional cameras were purchased to help Niagara Falls PD increase their crime fighting efforts in selected areas of their city. These cameras in Niagara Falls were located specifically in the Pine Avenue Business District to better address the crime problem located in this area. The cameras were requested by the Pine Avenue Redevelopment Project, which consists of local business owners that

DA Caroline Wojtasek cycling through Niagara Falls to Promote SafeCam Program.

work together to keep the area safe, clean, and inviting to their regular patrons and tourists. The group advocated for the cameras with the hope that they would supplement private security systems and increase crime prevention and assist with criminal prosecutions.

In June 2018, the District Attorney's Office knocked on doors throughout the Pine Avenue Business District. Augmented by volunteers from local businesses, block clubs and community police officers, the volunteers looked for video cameras that might be enrolled in the program. During the walk, they educated local business owners and managers about the value of the SafeCam program. It was an active day focused on crime and community safety, that culminated in the Niagara Falls Police Department's

> "Operation SafeCam has been a game-changer for Niagara County.

"Slow Roll" bicycle ride.

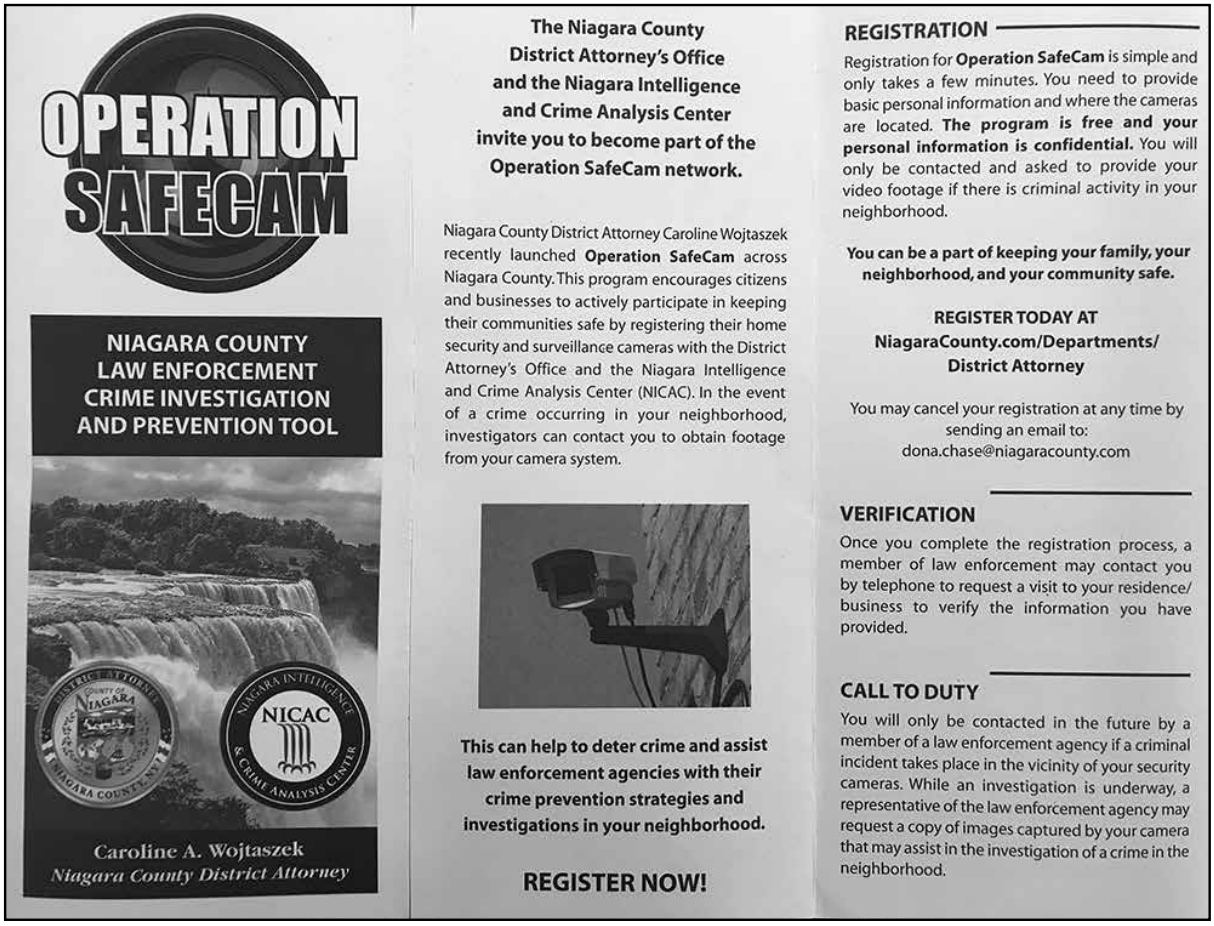
The cameras purchased by the District Attorney's Office using asset forfeiture funds will provide data directly to the Niagara Intelligence and Crime Analysis Center (NICAC). NICAC tracks crime hot spots and develops top criminal offender lists through data analysis to focus increased efforts on those who wreak havoc in the community.

Since its inception, the SafeCam program in Niagara County has been very successful. One recent success story concerns a murder case. In this case, the camera footage from a local gas station was recovered during the investigation. The video recorded the defendant, armed with a gun, approach the victim and shoot and kill the victim in broad daylight. Armed with the video footage of the incident, the defendant was successfully charged and convicted without having to rely on witness testimony. Historically, witnesses are reluctant to come forward and give information to the police for fear of retribution. Ultimately, the defendant was sentenced to twenty-five years in state prison because of the strength of the evidence.

"Operation SafeCam has been a game-changer for Niagara County. Through Operation Safecam we are joining forces with the community to improve and enhance our crime fighting tools. We also are sending the message that criminals are not welcome here and we will be watching. We will find you, we will arrest you, and will successfully prosecute you! It has changed how we investigate and prosecute our cases. I would encourage everyone to adopt the program and enjoy the benefit of greater community involvement and greater efficiency in prosecution of criminal cases," District Attorney Wojtaszek stated.

The author, Caroline Wojtaszek was elected Niagara County District Attorney in November 2016. Prior to her election, she worked for 6 years as the Confidential Law Clerk for Niagara County Court Judge Sara Sheldon and 12 years as a prosecutor for the Niagara County District Attorney's Office. As a Prosecutor in the Special Victims Unit, she earned convictions in several high- profile Niagara County cases.

Mrs. Wojtaszek earned her law degree from the State University at Buffalo and was head coordinator of the law school's Domestic Violence Task Force. She also worked as the Acting Domestic Violence Coordinator for Niagara County while attending law school. Prior to law school, Mrs. Wojtaszek graduated magna cum laude from the State University College at Brockport with dual majors in political science and sociology.



Finding Your Voice

BY CHIEF KEVIN SYLVESTER, OSSINING POLICE DEPARTMENT

When the Ossining Police Department began experimenting with social media, it wasn't completely authorized. Sure, the "team," two cops with a penchant for obscure internet humor, had asked the captain and he sort of gave permission. Whether or not the Chief completely understood what his people were up to is another issue. The fact that a formal social media policy wasn't implemented until more than a year later is a topic for a completely different article.

At its inception the department created a Facebook page but struggled to gain the attention of local residents. Most messages, factual yet boring, related to road closures and a handful of community outreach events. Long before we blamed an algorithm for all of our troubles, we were failing to reach residents all on our own. Aside from the fact that we had no training or equipment, we didn't understand the underlying structure of social media and how to gain attention of our target audience.

This is probably a good time to explain that our initiative wasn't a vain attempt to get famous. We knew that technology would allow us an opportunity to have unfiltered two-way communication with a mass audience. For free. In our experience, many police officers distrusted traditional media outlets. This was our chance to be reporters and get the story right. We were confident that we could take difficult information and share it in an easily digestible format, if only we could drop the "professional" front and start being ourselves.

> One of the foundational elements of our strategy was anonymity. No one person would be permitted to take credit for authoring our page.

If you get up in the morning and don the uniform, you likely made it through a selection process where one or more people opined that your disposition was sufficiently pleasant. If you're a chief, someone liked you on at least one day, and probably two or three. The point is that, as a police officer, you're trained to be "professional" but sometimes forget that, what got you in the door was your underlying personality. How does this relate to social media? We found that, when we quit using legalese and started pulling back the proverbial curtain, people paid attention. We believe that if we can draw you in with our charm, we can keep your attention when it's important.

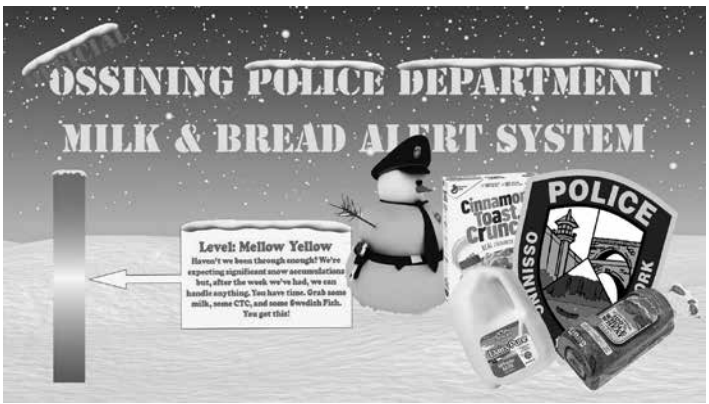
Some of the best times in a law enforcement career occur during shift change. Headquarters is full of cops and, if your job is anything like ours, the complaining is periodically broken by hearty belly laughs because our roster is loaded with some of the funniest human beings ever to wear a badge. Why then, should we be restricted to playing the straight man? Our social media posts began to reflect our collective personality. We carefully employed humor to help people accept the craziness, the sad, the outrageous, and even the awesomeness we saw on patrol.

One of the foundational elements of our strategy was anonymity. No one person would be permitted to take credit for authoring our page. People were left to wonder about the identity of the "social media cop." If we're being completely honest, the origin of that concept was born from a fear of failure. We weren't yet ready to sign our names and reputations away. Our forward facing strategy was to create a generalized persona for the Ossining Police Department. We like to believe that everyone played along when we asked them to politely inform residents that there is no single author but that the page was a true reflection of our staff. Social media established our voice and that voice became a brand. It created an expectation that our entire staff would be approachable, just like on Facebook. Some of our coworkers didn't like it. We didn't care.

When the former chief retired, I was chosen to replace him, essentially giving our social media team unlimited authority to speak on behalf of the Department. We began steaming full speed ahead. We published "Storytime," our version of the police blotter. In those articles, we describe an arrest from the previous day but more the way one cop would tell it to another. Most of those posts contain less facts than a traditional press release, and never feature a name or a mug shot. We believe in second chances and, in a tightly-knit community that would be nearly impossible if we publicized the face of every defendant. Notwithstanding, if you do something foolish, we're going to tell a cautionary tale for the benefit of your friends, family, and neighbors. The primary objective is to periodically remind our constituents that crime exists and that we're here to protect them. The feedback was incredibly positive. Oh, you caught someone stealing stuff from my neighbor's unlocked vehicle? Glad the OPD was there to catch him and I think I'll lock my doors! Success.

> The success or failure of your social media program turns on your ability to gain, and keep, the attention of your audience.

Ironically, our biggest gains come from weather reports. The Official Ossining Police Department Milk & Bread Alert System is a tongue in cheek reminder that, when it snows, your car will handle differently than on dry roads. Also, it's a polite reminder that you don't need to buy five gallons of milk the instant you see a flurry. If we're being completely honest, our Facebook page



— FINDING YOUR VOICE, continued on page 17

— FINDING YOUR VOICE, continued from page 16

occasionally doubles as a way for cops to say things they might not otherwise get away with. Is it silly? Sure, but it gets attention and, if we can draw you in with humor, you'll probably still be there during a critical incident.

Even more popular than telling people it's going to snow, is telling people that it's currently snowing. A common question during snow days is, "How are the roads? Can I drive yet?" I stand on Main Street, live, in the middle of a storm, with the exact same message every year, "It's snowing. Stay off the roads if you can. If you must drive, leave extra room between you and the car in front of you." People listen and some of them are your residents. All too frequently we receive messages that say, "I wish my department communicated like this." Your community is waiting to hear from you.

Critics have argued that personalizing our police department would somehow make us less effective. There isn't a statistic that can appropriately test that theory but, anecdotally, our digital following has grown exponentially. We have expanded our social media presence to include Instagram, multiple Twitter accounts, and Nextdoor. Each platform has its own unique purpose and personality. We like to believe that consistently increasing attendance at our live community events is directly related to our social media initiative.

The success or failure of your social media program turns on your ability to gain, and keep, the attention of your audience. Whether its humor or "just the facts," you have to ensure people come back so that you have their attention during critical incidents. Our system may not be right for everyone, but it works in our community. It's time for you to find your voice.

The Allure of FirstNet

BY CHIEF JAMES SUITOR, TOWN OF NIAGARA POLICE DEPARTMENT

Chief James Suitor

At 54 years old, I am currently in my 32nd year in law enforcement and for most of my "adult" life I've served in public safety as a volunteer fireman, a commercial ambulance paramedic, and for the past 16 years, as police chief. I'm proud to have served in the three branches of "traditional" public safety. Each has its own unique challenges and yet they have one thing in common: The need for interoperable voice & telecommunications (data) technology.

There was a time for most of us, nestled in our own municipalities, that our LMR (Land Mobile Radio) systems were "adequate." Adequate, meaning that coverage was marginal but we could talk to other public safety agencies when needed. That is how I would describe my department's old LMR. In fact, that's how I would describe my county from the 1970's through the early 2000's. Depending on the municipality, Niagara County had VHF low band for fire, VHF high band for law enforcement and a mix of UHF in the cities and for hospitals. They were Simplex systems with a few lucky enough to have repeaters and voting receivers. Mobile coverage was fine, portable coverage was "iffy." To overcome the inability to talk to adjacent agencies, some departments had multiple mobile radios in their vehicles. If you were lucky enough to have a technologically savvy police chief (that's me) you had cross banding mobiles turned into base stations and mobile vehicular repeaters using "out of band" portable radios capable of channel steering. It was a complicated way to interconnect systems. Almost everyone else in our county used their dispatch centers to relay information in an emergency. It was archaic and inefficient but was the reality for many municipalities throughout Western New York. The status quo was our reality because newer LMR technology was expensive & realistically out of reach, and then came September 11th, 2001.

> The status quo was our reality because newer LMR technology was expensive & realistically out of reach, and then came September 11th, 2001.

Interoperability quickly became one of the new "buzz" words for public safety. Simply put, the goal was to seamlessly interconnect public safety LMR (voice & data) between agencies. I remember the numerous articles, local and regional committee meetings, seminars, product testing and sales pitches bent on achieving this allusive "interoperability" goal.

In 2005, New York State leaders "floated" the idea of building a state-wide public safety voice communications system with the goal of interoperability. It was called SWN (Statewide Wireless Network). Western New York was chosen to be the first build out site (of 5 I believe) and was promised portable to portable coverage from my town in Niagara County to someone in NYC if needed. I was optimistic about the technology but naïve about the politics. I couldn't think of a scenario in which I wanted to talk to someone on a portable in New York City, but I could envision a need regionally in WNY. After a few years of engineering and testing, SWN didn't work out. Locally, after many more committee meetings, Niagara County decided on a limited regional approach to interoperability.

> And, there lies the ultimate reality problem of interoperability – money! Let's be painfully honest, there are more have not than have agencies in this state.

Fast forward to 2014, and after some hard lessoned learned nationally, Niagara County began building out an elaborate P-25 UHF phase II compliant trunking LMR system using multi-band radios to achieve our version of interoperability. It was housed at the Niagara County Sheriff's Office and it included most of the county PSAP's being transitioned into a central dispatching model. In all, the cost of the system was about $15 million dollars with most of the money coming from interagency cooperation (there were some fights) and lots of grant funding. And, there lies the ultimate reality problem of interoperability – money! Let's be painfully honest, there are more have not than have agencies in this state. Only a very small percentage of public safety agencies can afford even a limited attempt at interoperability and even less can afford the funding to keep it operational. There is however optimism for cost effective interoperability on the horizon and it is called FirstNet.

WHAT IS FIRSTNET?

On February 22, 2012, under the "Middle Class Tax Relief and Job Creation Act" of 2012, Congress created an independent authority under the Department of Commerce. This newly created federal agency was named the First Responder Network Authority (FirstNet Authority). Its task was to establish a Nationwide Broadband Network dedicated to First Responders. Following ▶

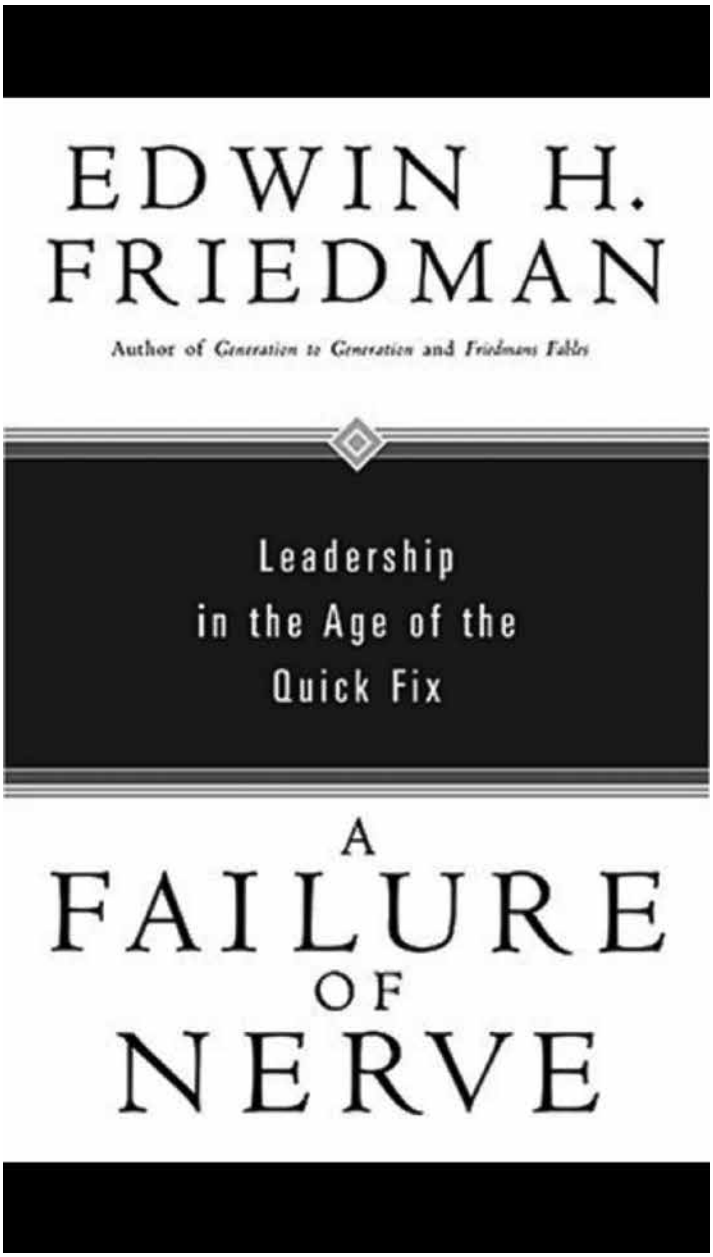
a comprehensive RFP process, AT&T was awarded a 25-year contract to establish the network, deploy, operate and maintain it.

On December 28th, 2017, Governor Cuomo announced that New York State would be joining FirstNet. The Governor stated, "During emergencies and disasters, every second counts, and ensuring our first responders have the tools they need during a crisis is vital to the safety and security of all New Yorkers." The entire state, from the Great Lakes to the most remote areas of the Adirondacks to New York City, must have seamless communication for our public safety community so that they can get more information quickly, make better informed decisions, and save lives." (https://www.governor.ny.gov/news/governor-cuomo-announces-new-york-states-participation-firstnet-first-responder-network)

Unless you've been following the progression of wireless technology and FirstNet, you might be asking yourself, "What does a wireless network access have to do with interoperability?" My response is simple, "Everything!"

In future articles we will explore how to locally leverage the maximum benefits of FirstNet by interfacing it with your local LMR systems. We will look at FirstNet's impact on the end user, from adding Smart Phones into your existing LRM systems and the plethora of smart phone applications in law enforcement. Like the promises of SWN, you might be able to use your portable to talk to another portable in NYC or, you could very possibly just use your smart phone, tablet or, Apple watch.

About the author: Chief Suitor is a 32 year veteran of law enforcement and has been Chief of Police in the Town of Niagara for the past 17 years.



Book Review

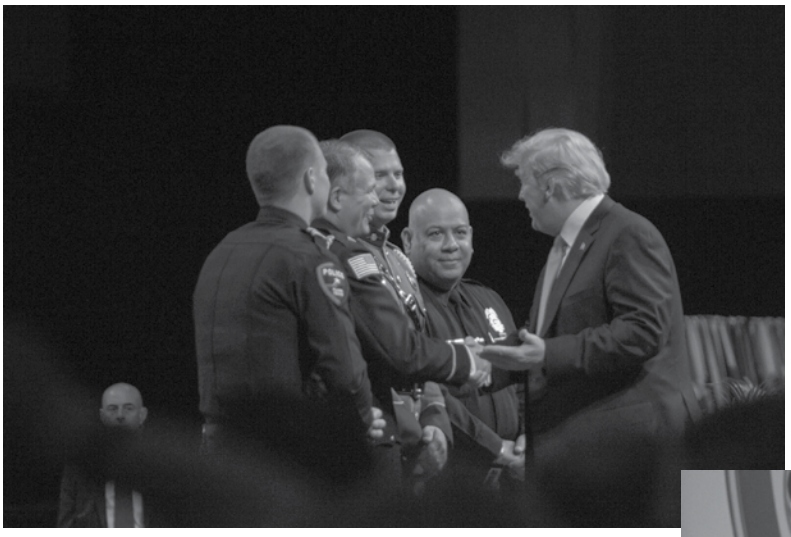
I found this book an excellent read for those seriously interested in leadership in the 21st century. Friedman's overall explanation that leadership hinges on the ability of the leader to understand the emotional processes that can affect leadership judgement is very compelling. If you examine the process, every family or institution has an emotional/relationship component. The challenge for an effective leader, according to Friedman, is the leader's ability to discern and navigate the emotional and relational climate of the family or organization – essentially become the "adult in the room"! As such, a good leader must focus on their own presence and bearing. Instead of reacting to emotional stimulus, a good leader must have a calm and steady presence to transform anxiety into productive energy.

An interesting takeaway from the book is that a real problem of leadership today may not be the lack of education, information, or skill of a leader. I think most people who ascend to a leadership position have the requisite education and skills. Rather, the problem may be a "failure of nerve!" This failure is because many leaders may lack the nerve to stand firm while being exposed to other people's emotional anxiety and reactivity. Overall, I think the ideas and thoughts presented by the author are applicable in today's leadership environment and well worth the read.

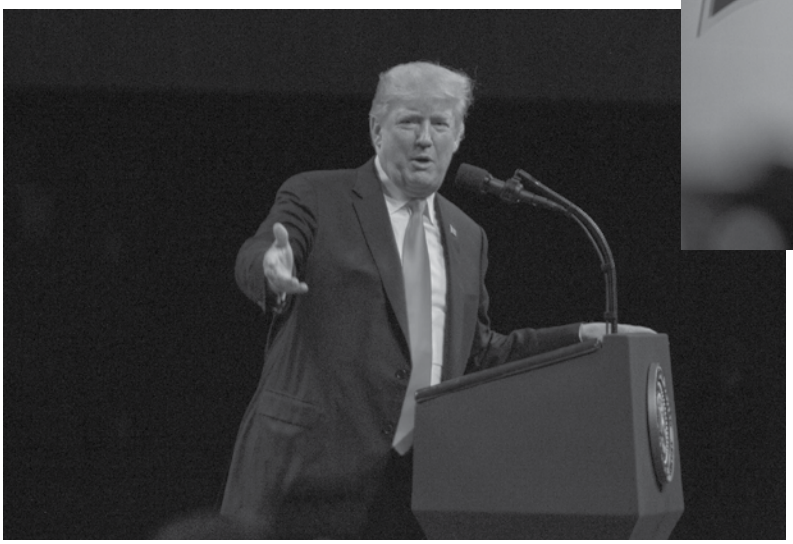
Edwin Friedman (d. 1996) served for 20 years as a pulpit rabbi and for 25 years as an organizational consultant & family therapist in the Washington DC area. He also served in the Lyndon Johnson administration. His unique experience allowed him to observe leadership – and its problems – in the family, the church, and the political sphere.

Members of the Westchester County Chief's Association with Chief Kevin Sylvester after Chief Sylvester's presentation "How to start a Social Media presence from scratch" at IACP.

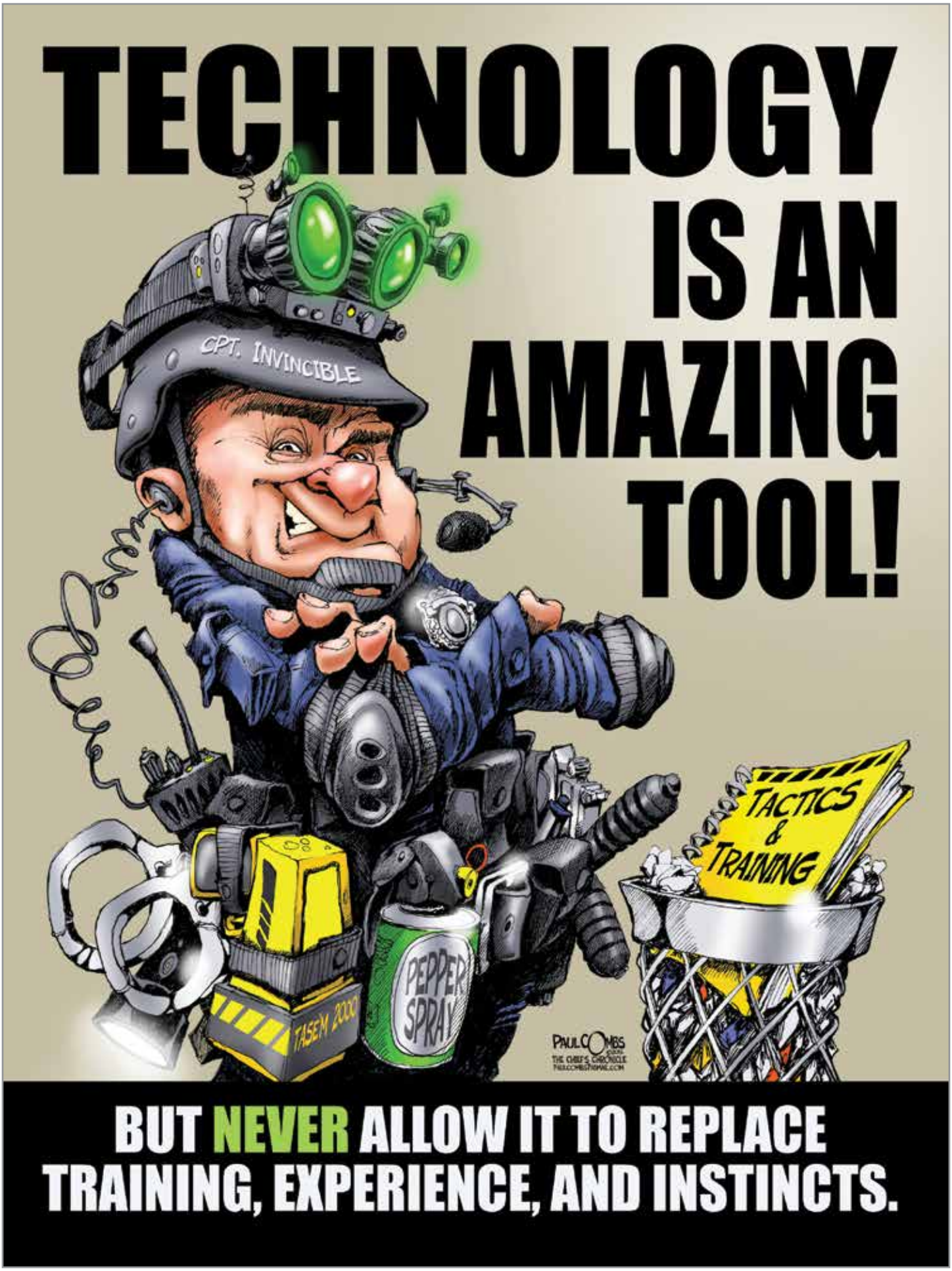
Pictured from left to right; Chief Anthony Piccolino, Chief John Costanzo, Commissioner Shawn Harris, Chief Paul Olivia, Chief Kevin Sylvester, Chief Michael Cerone, Chief Russell Harper and Chief Greg Austin.



President Trump congratulating the IACP Medal of Honor recipients.



IACP picture 2018 President Trump Courtesy of Chief Greg Austin


TECHNOLOGY
IS AN
AMAZING
TOOL!
CPT. INVINCIBLE
TACTICS
&
TRAINING
PEPPER
SPRAY
TASER 2000
PAUL COMBS
BUT NEVER ALLOW IT TO REPLACE
TRAINING, EXPERIENCE, AND INSTINCTS.

NEW YORK STATE ASSOCIATION
OF CHIEFS OF POLICE, INC.
2697 HAMBURG STREET
SCHENECTADY, NY 12303

New York State Association of Chiefs of Police

–Save the Date–

Annual Training Conference
July 21 - July 24, 2019

Hyatt Regency Rochester
125 East Main Street
Rochester, New York

HYATT
REGENCY
ROCHESTER