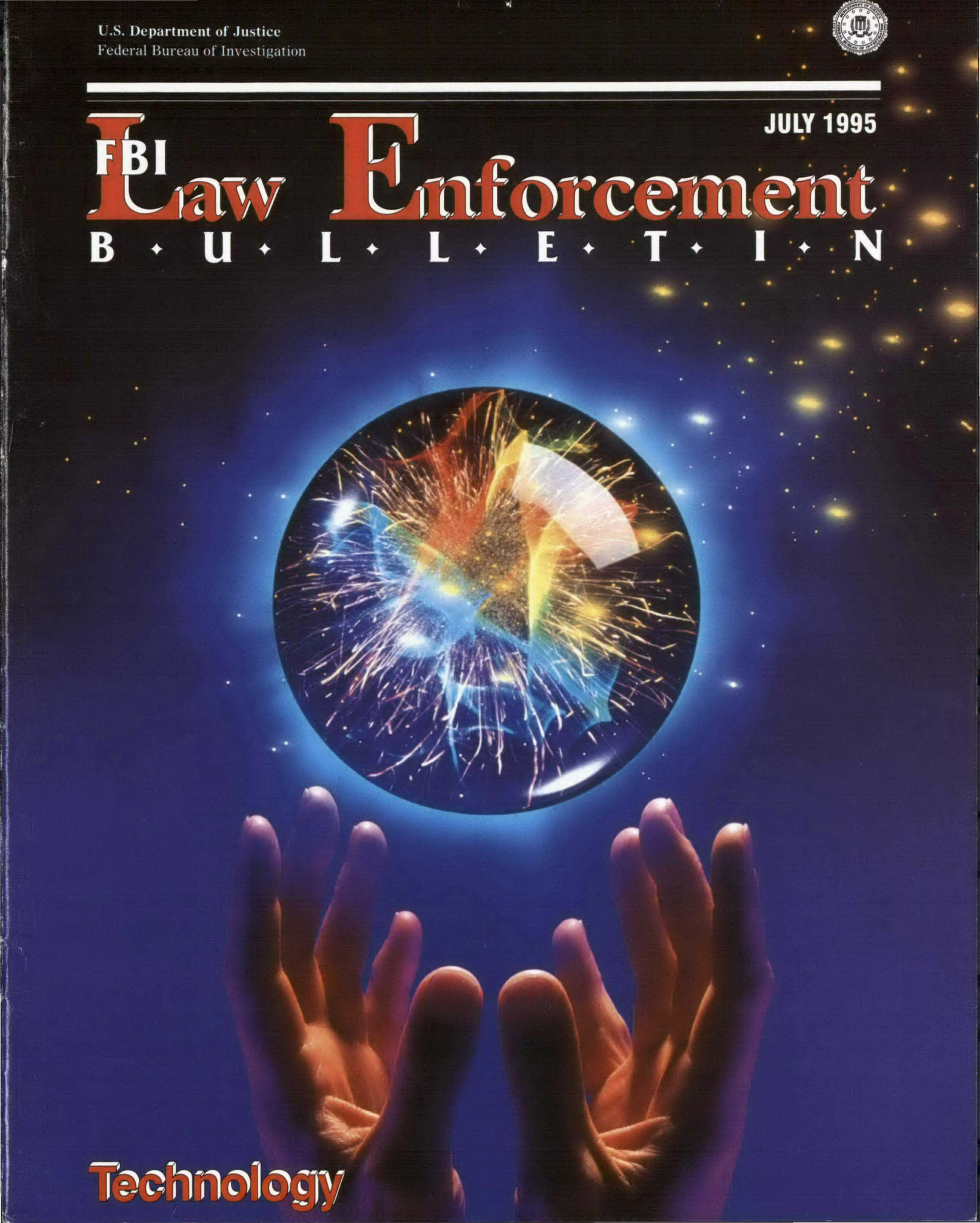
U.S. Department of Justice
Federal Bureau of Investigation

JULY 1995

FBI Law Enforcement B·U·L·L·E·T·I·N



Technology

July 1995
Volume 64
Number 7

**United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535**

**Louis J. Freeh
Director**

Contributors' opinions and statements should not be considered as an endorsement for any policy, program, or service by the FBI.

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget.

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, FBI Academy, Quantico, VA 22135.

Editor
Stephen D. Gladis, Ph.D.
Managing Editor
Kathryn E. Sulewski
Art Director
John E. Ott
Associate Editors
Andrew DiRosa
Julie R. Linkins
Kimberly J. Waggoner
Assistant Art Director
Brian K. Parnell
Staff Assistant
Stephanie L. Lowe

Internet Address:
fbileb@justice.usdoj.gov

Cover photo
© The Image Bank

FBI Law Enforcement B•U•L•L•E•T•I•N

Features

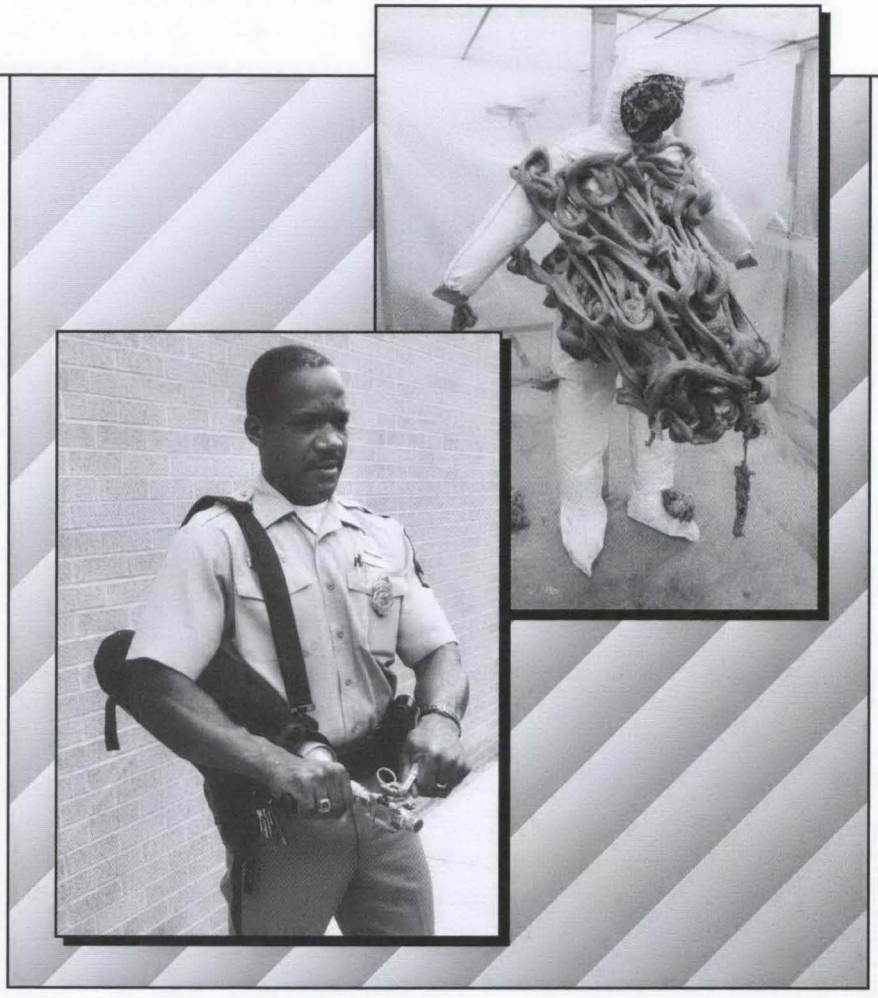
Focus on Technology

Departments

ISSN 0014-5688 USPS 383-310

On the Cutting Edge
Law Enforcement Technology

By DAVID G. BOYD, M.B.A.



In 1972, a researcher from the U.S. Department of Justice's National Institute of Justice (NIJ) stumbled upon heavy-duty military tires made from a fiber that could stop bullets. This material, perhaps best known by its trademark Kevlar, weaved its way into the soft body armor worn by law enforcement personnel. Since 1975, when NIJ first conducted field tests in 15 cities across the country, bulletproof vests have saved the lives of thousands of police officers.

Today, discoveries like this do not happen by accident. Rather, an agreement between the Department of Justice (DOJ) and the Department of Defense (DOD) ensures that the high-tech wizardry once employed solely by the military will be used to enhance the capabilities of law enforcement. As a sign of their commitment, the departments have formed an office whose mission is to move law enforcement into the 21st century.

THE NATIONAL LAW ENFORCEMENT TECHNOLOGY CENTER

DOJ made a commitment to develop new technologies for law enforcement long before its April 1994 Memorandum of Understanding with DOD. Under the auspices of the NIJ, the Technology Assessment Program Information Center (TAPIC) had been setting performance standards for equipment, testing new products, and disseminating test results to criminal justice agencies since 1968.

TAPIC eventually changed its name, but not its basic mission. The new National Law Enforcement Technology Center (NLETC) will continue to help develop the technology that law enforcement officers need to stay several steps ahead of criminals.

A COOPERATIVE EFFORT

NLETC works with several other government agencies to accomplish its objectives. First, DOD's Advanced Research Projects

Agency (ARPA) identifies "dual-use" technologies—those that could have both military and law enforcement applications.

Next, NLETC's Advisory Council, a group of more than 80 senior Federal, State, and local law enforcement officials from the United States and Canada, meets twice-yearly to prioritize the projects identified by ARPA. Products that protect human lives, save agency resources, or decrease the potential for liability claims against an agency usually receive top priority.

The advisory council recommends such projects for NIJ funding. It also serves as a "reality check," noting which applications would fail to meet the requirements of law enforcement officers in real-world situations.

In conjunction with the National Institute of Standards and Technology's Office of Law Enforcement Standards, the advisory council sets the standards to which the equipment must adhere. Standardization involves establishing criteria and testing procedures to evaluate whether the product or procedure meets the performance requirements of the law enforcement officers who will use it. Council members establish criteria with an administrator's eye—one that often sees dollar signs. Accordingly, the cost of new technology should not exceed its benefits to law enforcement.

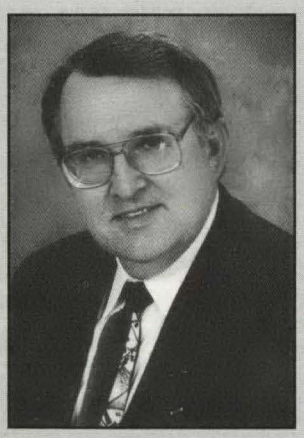
PRODUCT DEVELOPMENT AND TESTING

With projects identified, prioritized, and standardized, NLETC disseminates the council's reports to research and development concerns in NIJ, DOD, and private industry. In turn, these entities create solicitations, which outline the projects for which NIJ will provide funding. NIJ then accepts proposals from manufacturers and laboratories interested in developing and testing the equipment and awards grants to the firm whose proposal best meets the previously established standards.

By this time, several years likely have passed. Developing and testing a prototype in the laboratory and then in the field take considerably more time. However, the time spent is well worth the effort if it means safer, more effective products. Furthermore, once NIJ sets standards for a product or technique, other agencies—both public and private—can use the criteria to develop new or improved products.

Finally, with testing complete, NLETC analyzes the data and disseminates the results. It continues to publicize the information gathered just as TAPIC did in the past: Through articles in criminal justice publications, in technology bulletins, at criminal justice conferences, and in its newsletter, newly christened *Technology Beat.*

The new center also is a place where researchers, manufacturers, and practitioners can meet to exchange information. Indeed, NLETC will make available "state-of-the-science" technologies to benefit law enforcement officers across the country. Many new products and procedures—some of which are described here—already await the law enforcement seal of approval.



"Less-than-lethal technologies that save the lives of innocent people and protect agencies from liability lawsuits represent an important area of research."

Mr. Boyd is the Director of Science and Technology at the National Institute of Justice, U.S. Department of Justice, Rockville, Maryland.

LESS-THAN-LETHAL TECHNOLOGIES

Developing less-than-lethal technologies represents a top priority for law enforcement. In a 1985 landmark decision, the Supreme Court ruled that deadly force is unjustified against an escaping, nonviolent felon[1] and called for the law enforcement community to develop

appropriate equipment to apprehend suspects safely.

In 1986, the Attorney General's Conference on Less-Than-Lethal Weapons characterized the law enforcement officer's most common tools—the nightstick and the gun—as inappropriate in many instances, especially in hostage and barricade situations, which require equipment that can stop a dangerous subject without endangering innocent hostages or bystanders. Clearly, criminal justice professionals need new approaches to capturing, subduing, and detaining subjects.

Sticky Foam

One product under development is restraining or "sticky" foam, a taffy-colored, gel-like substance that, when dispersed from a pressurized shoulder-slung "gun," expands and turns into a glue that sticks on contact. The Department of Energy developed it to help secure nuclear weapon facilities by tripping up and entangling trespassers. It originally was believed that police officers could shoot the foam from a safe distance to stop fleeing suspects or to disable violent individuals armed with weapons other than guns.

Unfortunately, laboratory tests on volunteer subjects showed that the fairly large quantities required to achieve disabling effects made cleanup difficult. Despite this drawback, the U.S. Marines expressed an interest in sticky foam and have used it successfully during recent peacekeeping operations in Somalia.

In addition, the foam may prove effective in quelling prison disturbances by denying inmates access to certain areas, as may aqueous foam, a kind of thick, artificial fog. Tests and evaluations continue on these products, as NLETC explores their safety and effectiveness.

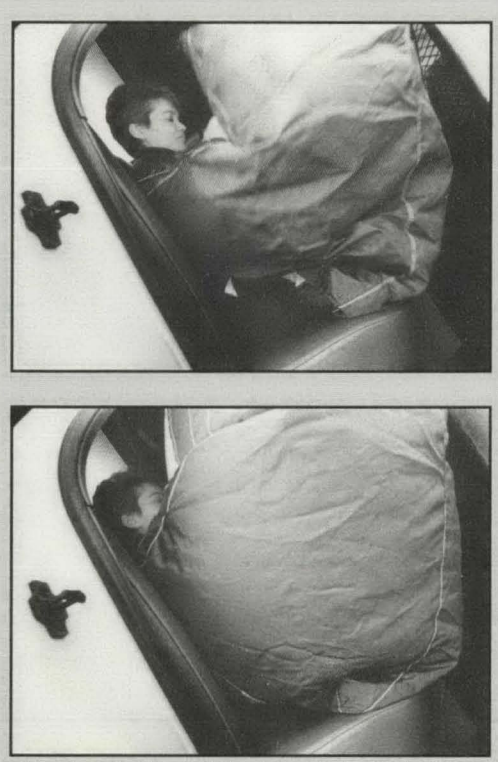
Strobe-and-Goggle Technology

Already in the prototype stages, strobe-and-goggle technology employs a bright flashing light to blind and disorient subjects during drug raids or assaults on barricaded structures, allowing officers to enter the premises. In the past, these pyrotechnic flash-light generators, or "flash-bang" devices, had limitations. They sometimes generated extreme amounts of heat and light. Most often, they disoriented subjects for too brief a time. Worse, the officers who used them experienced the same effects as the criminals.

The new prototype includes goggles that protect law enforcement officers from the light's effects. In this case, the technology needed to make the goggles already existed. Both military pilots and commercial welders wear goggles designed to darken when exposed to bright light.

Backseat Airbag

New patrol cars have driver-side and passenger-side airbags, but soon they may have backseat airbags as well. With the ability to activate and control the bag from the front seat, an officer could subdue an unruly subject without harm to the individual. These bags also could be used in prisons to control and, if necessary, immobilize unruly prisoners. A similar technology might expel unwilling detainees from their cells.



A backseat airbag inflates to restrict a subject's mobility.

Remote-Control Barrier Strips

Law enforcement agencies face a myriad of potential liability situations. Many such lawsuits spring not from the use of firearms but from high-speed vehicular chases. In California last year, more than 7,000 high-speed pursuits occurred. One out of five ended in accidents, resulting in more than 1,200 injuries.[2] About 1 percent of all high-speed chases end with a fatality.[3]

In response to the need for safe ways to stop fleeing suspects, a national laboratory is developing technology to allow police to activate, by remote control, strips of needles that pop out of the road and puncture the tires of fleeing vehicles. Then, the police will retract the needles to chase the subject. The ability to activate the system remotely will prevent injury to law enforcement and to innocent civilians. NLETC anticipates evaluating a prototype strip some time in 1995.

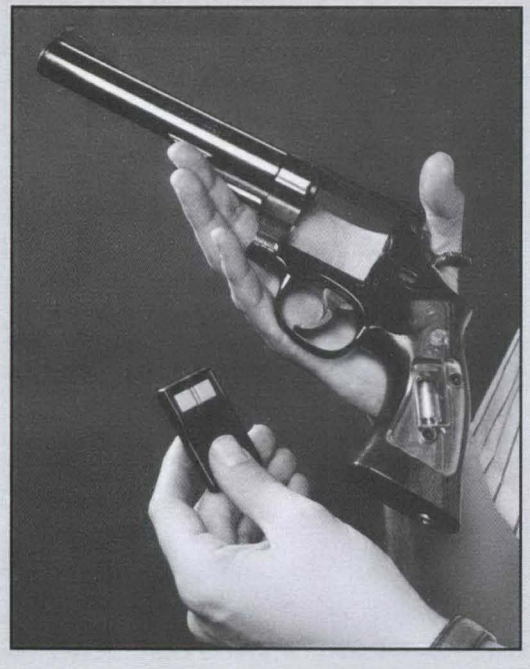
Fleeing Vehicle Tagging System

Ultimately, if law enforcement cannot find a harmless way to stop a pursued vehicle, it happily will settle for a way of definitively marking the vehicle to locate it at a later time. The same laboratory developing retractable spiked strips is at work on a projectile launcher system, which would allow officers to fire a "tagging" projectile at a fleeing vehicle. Equipped with a tiny radio transmitter, the object would stick to the car and allow police to track the vehicle from a safe distance without endangering lives or allowing the suspect to escape.

OFFICER SAFETY

Less-than-lethal technologies that save the lives of innocent people and protect agencies from liability lawsuits represent an important area of research. However, officer safety remains a top priority, and NLETC continues to sponsor projects designed to save officers' lives.

This prototype of the "smart gun" has a sensor built into the handgrip that prevents unauthorized users from firing the weapon.



Smart Gun

One-sixth of all law enforcement officers killed each year are shot with their own weapons.[4] A national laboratory is testing a variety of sensors, which, when placed in the handgrip of a weapon, would "recognize" the authorized user and refuse to fire for anyone else. The resulting "smart gun" never could be used against its owner.

In addition to saving the lives of law enforcement officers, smart guns might save the lives of children who kill themselves, either accidentally or intentionally, with their parents' weapons. Finally, criminals who obtain weapons illegally could not fire them.

Personnel Monitoring System

Technology soon may make the standard police walkie-talkie obsolete. Originally developed for Army medics, a personnel monitoring system will enable law enforcement and other public service personnel to remain in direct contact with their departments at all times.

A miniature camera transmits full-color video of the scene; wireless networks allow audio communication and data transmissions; a Global Positioning System provides the officer's exact street location; and a personal status monitor tracks the officer's vital signs. As a result, an agency could locate and monitor an officer in distress, quickly assess the situation, and respond accordingly.

INVESTIGATIVE TOOLS

The "perfect crime" becomes harder to commit every day. Emerging technology allows law enforcement officers to piece together crime scene clues where little evidence appears to exist.

The Magic Wand

In only 18 months and with a research grant of under $100,000, the Alaska Crime Laboratory, together with a nationally known private firm, developed and distributed the Fingerprint Visualization System, named the "Magic Wand." It allows investigators to lift prints from nonporous surfaces at the scene of the crime, not in the lab.

It helps police identify and apprehend suspects quickly.

The Fingerprint Visualization System allows prints to be developed onsite in a matter of seconds using a portable, handheld device that combines a superglue with a dye and reduces the procedure to one simple step. With prints in hand, the investigator need only link them to a suspect, a process that one day will be accomplished from the officer's patrol vehicle.

Smart Car

Firefighters and mail carriers use specially designed trucks on the job; yet, no vehicles have been designed specifically for police work. Even cars with "police packages" usually come equipped only with different paint, special lighting packages, and other accessories. With limited buying power, law enforcement could not even persuade Detroit automobile manufacturers to produce cars without passenger-side airbags, which, if deployed, could turn equipment mounted on the passenger side into dangerous projectiles.

Still, some private firms that once held DOD contracts now have focused their creative energies on law enforcement. Police vehicles have become fertile ground for the seeds of science and technology. The "smart car," already being used by the Anne Arundel County, Maryland, Police Department and the Maryland State Police, is ready to merge onto the information superhighway with computer hardware and software designed to link officers on the street with databases all over the country.

These systems allow officers to do more than write reports on computers. They provide immediate access to wants and warrants information, letting officers know what dangers they might face before they even step from their patrol cars.

The computers also permit on-the-spot transmission and retrieval of arrest records, fingerprints, and mugshots. Some day, they will hold voice samples, giving law enforcement officers a complete offender profile from the street. As departments acquire more smart cars and network them so that they communicate with one another, a trip to the station may be a rare occurrence for police officers in the future.

> ***"...NLETC will make available 'state-of-the-science' technologies to benefit law enforcement officers across the country."***

CONCLUSION

Small police departments usually do not have the resources to implement new techniques and technologies for fighting crime. Even larger departments with the funds may not have access to the information they need to make the right purchases. In fact, law enforcement agencies as a group do not possess the buying power to encourage manufacturers to research and develop products their officers need at prices they can afford.

Adapting technology to serve in a field different from the one for which it was intended frequently costs almost as much as developing it from scratch. Multiple-use technologies save money by targeting several fields, including the military, public service, and law enforcement. With the National Law Enforcement Technology Center, the Federal Government has reaffirmed its commitment to identifying, developing, and manufacturing new products and applications specifically designed with law enforcement in mind.

Technology cannot fix every shortcoming. It cannot make up for poor judgment or compensate for inadequate or nonexistent training. It cannot fix the problems that result from poor officer screening or selection, and it can never replace competent leadership.

Technology can provide the tools to make law enforcement more efficient and effective, limit the consequences of poor judgment, and improve the safety of the police and the public. It can save lives.✦

Endnotes

[1] *Tennessee* v. *Garner*, 471 U.S. 1, 105 S.Ct. 1694.

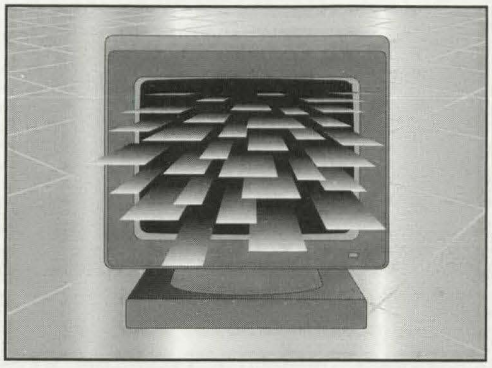
[2] Unpublished report by the California Highway Patrol.

[3] Studies have produced fatality estimates ranging from about .38 percent to 3 percent. *See* Geoffrey P. Alpert, "Police Pursuit and the Use of Excessive Force," unpublished paper; and Tim Grimmond, "Police Pursuits," *Police Chief*, July 1992, 43-47.

[4] Author-calculated average of Uniform Crime Reports data for the past 12 years.

For information on products or services offered by the NLETC, call 1-800-248-2742 or write NLETC, Box 1160, Rockville, MD 20849.

On the Line



E-mail Responses

The flood of messages we have received since publishing our e-mail address in February indicates many of our readers use the Internet and have much to discuss. We asked how computers have affected policing and how you use them in your departments. From the largest to the smallest, police departments across the country have felt the impact of the computer revolution.

A detective in a New Hampshire police department wrote that officers use computers for preparing embezzlement and check kiting cases for court, creating graphic displays of offenses to show juries, and simply for keeping the department's budget records. His and other departments use computer-aided design software to create crime and accident scene drawings.

An officer from a small department (3 full-time officers and 20 reserves) said that they use personal computers for all of their recordkeeping. The officers there initially resisted the technology, but now they "...would not think of writing a report without the computer."

Many members of the criminal justice community—police chiefs, dispatchers, patrol officers, students, and professors—have been exploring the Internet to find useful information. Some focus on researching the databases and documents available on the global network. Others concentrate on discussing current trends in law enforcement and exchanging information with criminal justice practitioners and researchers around the world. They use such computer bulletin board services (BBS) as the National Criminal Justice Reference Service (NCJRS*BBS), SEARCH, the International Association of Chiefs of Police IACP NET, the American Society of Law Enforcement Trainers (ASLET) portion of the CompuServe SafetyNet forum, and the FOPNet for members of the Fraternal Order of Police.

The most common question we received was, "What resources are out there that we can use?" Because, like many of you, we are just starting to explore the Internet, we would like to turn that question around and ask, "What resources have you found?" Some respondents have already provided us with good information, and we are compiling a list to make available to our readers.

Many of you thought that we were operating a bulletin board service or a listserv. We have not crossed that technological threshold yet and can only exchange e-mail messages via the Internet at this time.

Finally, some of our e-mail correspondents described a negative computer phenomenon that has touched their lives—crimes committed via computer. Reports from readers confirm recent news media accounts of pedophiles worming their way into the lives of innocent children by corresponding over the computer. Bank and investment fraud as well as con games of every variety can—and do—take place using computers.

Yet, criminals are not the only ones who can tap into the vast resources on the Internet. Law enforcement is finding innovative ways to combat these cybercriminals. Rapid communication over long distances among many jurisdictions works in the interests of law enforcement. We are interested in hearing about cases you have investigated or methods you use to detect and investigate computer-related crimes.

Most of our e-mail correspondents agreed that the Internet offers many benefits, even though some pointed out its current limitations. From participating in discussion groups among practitioners to locating documents about model programs implemented by other municipalities, members of the criminal justice community can use the Internet to continue to improve their performance, to enrich the profession, and to enhance their service to the public. ✦

Virtual Reality
The Future of Law Enforcement Training

By
JEFFREY S. HORMANN

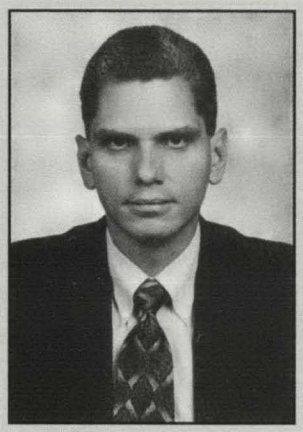
A late night police pursuit of a suspected drunk driver winds through abandoned city streets. The short vehicle chase ends in a warehouse district where the suspect abandons his vehicle and continues his flight on foot. Before backup arrives, the rookie patrol officer exits his vehicle and gives chase. A quick run along a loading dock ends at the open door to an apparently unoccupied building. The suspect stops, brandishes a revolver, and fires in the direction of the pursuing officer before disappearing into the building. The officer, shaken but uninjured, radios in his location and follows the suspect into the building.

Did the officer make a good decision? Probably not by most departments' standards. Whether the officer's decision proves right or wrong, the training gained from this experience is immeasurable, that is, provided the officer lives through it. Fortunately for this officer, the scenario occurred in a realistic, high-tech world called virtual reality, where training can have a real-life impact without the accompanying risk.

TRADITIONAL TRAINING LIMITATIONS

Experience may be the best teacher, but in real life, police officers may not get a chance to learn from their mistakes. To survive, they must receive training that prepares them for most situations they might encounter on the street. However, because many training programs emphasize repetition to produce desired behaviors, they may not achieve the intended results, especially after students leave the training environment. Thus, the more realistic the training, the greater the lessons learned.

Additionally, even some in law enforcement may fall prey to the effects of what has come to be termed "The MTV Generation."[1] As products of this generation, today's young officers purportedly have short attention spans requiring new, nontraditional training methods. The key to teaching this new breed is to provide fast-paced,



> ***"...virtual reality allows law enforcement officers to...react to real-world situations without the accompanying dangers."***

Chief Warrant Officer Hormann is the Special Agent in Charge of the Fort Belvoir Resident Agency, U.S. Army Criminal Investigation Command, Fort Belvoir, Virginia.

attention-getting instruction that is clear, concise, and relevant.[2]

TRAINING WITH VIRTUAL REALITY

Virtual reality can provide the type of training that today's law enforcement officers need. By completely immersing the senses in a computer-generated environment, the artificial world becomes reality to users and greatly enhances their training experiences.

Although considerable research and development have been conducted in this field, only a limited amount has applied directly to law enforcement. The apparent reason simply is that, for the most part, law enforcement has not asked for it.

Because virtual reality technology is relatively new, most law enforcement administrators know little about it. They know even less about what it can do for their agencies. By understanding what virtual reality is, how it works, and how it can benefit them, law enforcement administrators can become involved in the development of this important new technology.

WHAT IS VIRTUAL REALITY?

Simply stated, virtual reality is high-tech illusion. It is a computer-generated, three-dimensional environment that engulfs the senses of sight, sound, and touch. Once entered, it becomes reality to the user.

Within this virtual world, users travel among, and interact with, objects that are wholly the products of a computer or representations of other participants in the same environment. The limits of this virtual environment depend on the sophistication and capabilities of the computer and the software that drives the system.

HOW DOES VIRTUAL REALITY WORK?

Based on data entered by programmers, computers create virtual environments by generating three-dimensional images. Users usually view these images through a head-mounted device, which can be a helmet, goggles, or other apparatus that restricts their vision to two small video monitors, one in front of each eye. Each monitor displays a slightly different view of the environment, which gives users a sense of depth.

Another device, called a position tracker, monitors users' physical positions and provides input to the computer. This information instructs the computer to change the environment based upon users' actions. For example, when users look over their shoulders, they see what lies behind them.

Because virtual reality users remain stationary, they use a joy stick or track ball to move through the virtual environment. Users also may wear a special glove or use other devices to manipulate objects within the virtual environment. Similarly, they can employ virtual weapons to confront virtual aggressors.

To enhance the sense of reality, some researchers are experimenting with tactile feedback devices (TFDs). TFDs transmit pressure, force, or vibration, providing users with a simulated sense of touch.[3] For example, a user might want to open a door or move an object, which in reality, would require the sense of touch. A TFD would simulate this sensation. At present, however, these devices are crude and somewhat cumbersome to use.

USES FOR VIRTUAL REALITY

In today's competitive business environment, organizations continuously strive to accomplish tasks faster, better, and

inexpensively. This especially holds true in training.

Virtual reality is emerging rapidly as a potentially unlimited method for providing realistic, safe, and cost-effective training. For example, a firefighter can battle the flames of a virtual burning building. A police officer can struggle with virtual shoot/don't shoot dilemmas.[4]

Within a virtual environment, students can make decisions and act upon them without risk to themselves or others. Instructors can critique students' actions, enabling students to review and learn from their mistakes. This ability gives virtual reality a great advantage over most conventional training methods.

Military Training

The Department of Defense (DOD) leads public and private industry in developing virtual reality training. Since the early 1980s, DOD has actively researched, developed, and implemented virtual reality to train members of the armed forces to fight effectively in combat.

DOD's current approach to virtual reality training emphasizes team tactics. Groups of military personnel from around the world engage in combat safely on a virtual battlefield. Combatants never come together physically; rather, simulators located at various sites throughout the world transmit data to a central location, where the virtual battle is controlled. Because it costs less to move information than people, this form of training has proven quite cost-effective.

An additional benefit to this type of training is that battles can be fought under varying conditions. Virtual battlefields re-create real-world locations with interchangeable characteristics. To explore "what if" scenarios, participants can modify enemy capabilities, terrain, weather, and weapon systems.

Virtual reality also can re-create actual battles. Based on information from participants, the Institute for Defense Analyses re-created the 2nd Armored Cavalry Regiment Offensive conducted in Iraq during Operation Desert Storm. The success of the virtual re-creation became apparent when, upon viewing the simulations, soldiers who had fought in the actual battle reported the extreme accuracy of the event's depiction and the feeling of reliving the battle.[5] Clearly, virtual reality holds great potential for accurate review and analysis of real-world situations, which would be difficult to accomplish by any other method.

> ***"...virtual reality holds great potential for accurate review and analysis of real-world situations, which would be difficult to accomplish by any other method."***

Preliminary studies show that military units perform better following virtual reality training.[6] Even though virtual environments are only simulations, the complete immersion of the senses literally overwhelms users, totally engrossing them in the action. This realism presumably plays a major role in the program's success and likely will prove positive in future endeavors. In fact, due to its success in training multiple participants in group combat situations, DOD plans to train infantry personnel individually with virtual reality fighting skill simulators.[7]

Law Enforcement Training

While virtual reality has proven its value as a training and planning tool for the military, applications for this technology reach far beyond DOD. To varying degrees, many military uses can transfer to law enforcement, including training in firearms, stealth tactics, and assault skills.

Unfortunately, few organizations have dedicated resources to developing virtual reality for law enforcement. According to a recently published resource guide, more than 100 companies currently are developing and/or selling virtual reality hardware or software. However, none of these firms mentioned law enforcement uses.[8]

Further, a review of relevant literature revealed numerous articles on virtual reality technology, but only a few addressed law enforcement applications. Yet, virtual reality clearly offers law enforcement benefits in a number of areas, including pursuit driving, firearms training, high-risk incident management, incident re-creation, and crime scene processing.

Pursuit Driving

Pursuit driving represents one area in which a virtual reality

application has become reality for law enforcement. Law enforcement personnel identified a need and provided input to a well-known private corporation that developed a driving simulator equipped with realistic controls.

The simulator provides users with realistic steering wheel feedback, road feel, and other vehicle motions. The screen possesses a 225-degree field of view standard, with 360-degree coverage optional. Simulations can involve one or more drivers, and environments can alternate between city streets, rural back roads, and oval tracks. The vehicle itself can change from a police car to a truck, ambulance, or a number of others.

Virtual reality driving simulators provide police departments invaluable training at a fraction of the long-term cost of using actual vehicles. In fact, the simulator is being used by a number of police departments around the country.

During the past year, the Los Angeles County Sheriff's Office Emergency Vehicle Operations Center (EVOC) has used a four-station version of the driving simulator to train its officers. The simulators help students develop judgment and decisionmaking skills, while providing an environment free from risk of injury to students or damage to vehicles. Still, as the EVOC supervisor cautions, virtual reality training should complement, not replace, actual behind-the-wheel instruction.[9]

Firearms Training

Virtual reality could greatly enhance shoot/don't shoot training simulators currently in use, such as the Firearms Training System, a primarily two-dimensional approach that possesses limited interactive capabilities. A virtual reality system would allow officers to enter any three-dimensional environment alone or as a member of a team and confront computer-generated aggressors or other virtual reality users.

Evaluators could observe the training from any perspective, including that of the officers or the aggressors, or from any other location in the environment. Training scenarios could involve actual building floor plans or local city streets, and criteria such as weather, number of participants, or types of weapons could be altered easily.

High-Risk Incident Management

In addition to weapons training, virtual reality could prove invaluable for SWAT team members before high-risk tactical assaults. Floor plans and other known facts about a structure or area could be entered into a computer to create a virtual environment for commanders and team members to analyze prior to action.

Incident Re-Creation

Law enforcement agencies could collect data from victims, witnesses, suspects, and crime scenes to re-create traffic accidents, shootings, and other crimes. The

Key Terms

Virtual Image: An image observed even though no concrete object exists. A reflection in a mirror is an example of a virtual image.

Virtual Display: Visual, auditory, and tactile images that, like virtual images, do not actually exist.

Virtual Reality: An environment created by projecting visual, auditory, and tactile images into the eyes. With the senses immersed in these images, users perceive this environment as reality.

Virtual Common or Virtual Community: The virtual environment where virtual reality users "meet."

Cyberspace: The network of virtual reality users interfacing in a virtual community.

Source: Carmen Miller, "Online Interviews Dr. Thomas A. Furness, III, Virtual Reality Pioneer," Online, *November 1992, 14.*

virtual environment created from the data could be used to refresh the memories of victims and witnesses, to solve crimes, and ultimately, to prosecute offenders.

Crime Scene Processing

Virtual reality crime scenes could be used to train both detectives and patrol officers. Students could search the site and retrieve and analyze evidence without ever leaving the station. Actual crime scenes could be re-created to add realism to training or to evaluate prior police actions.

IS VIRTUAL REALITY VIRTUALLY PERFECT?

Though virtual reality may appear to be the ideal law enforcement tool, as with any new technology, some drawbacks exist. Currently, areas of concern range from cumbersome equipment to negative physical and psychological effects experienced by some users. Fortunately, however, the field is evolving and improving constantly, and as virtual reality gains widespread use, most major concerns should be dispelled.

Physical Limitations and Effects

Because computers currently are not fast enough to process large amounts of graphic information in real time, some observers describe virtual environments as "slow-moving."[10] The human eye can process images at a rate much faster than a computer can generate them. In a virtual environment, frames are displayed at a rate of about 7 per second, an extremely slow speed when compared to a television, which generates 60 frames per second.[11] Users find the resulting choppy or slow graphics less than appealing.

Slow graphics also produce a phenomenon known as simulator sickness. Some virtual reality users experience disorientation and nausea somewhat akin to motion sickness. Simulator sickness occurs because the eyes are accustomed to real-world speed; virtual reality's slower graphics negatively affect about 8 to 10 percent of all users. However, as the motion more closely mimics real-time speed, fewer people will experience such ill effects.[12]

> ***"Virtual reality is emerging rapidly as a potentially unlimited method for providing realistic, safe, and cost-effective training."***

Another equipment shortfall is the head-mounted device (HMD). In general, HMDs are large and awkward, and many users find them uncomfortable. Although virtual reality innovators generally view this as a relatively minor problem, they are working to improve design.

One HMD currently under development compares in size and shape to a pair of sunglasses. Rather than using small video monitors, the glasses contain laser-imaging equipment that projects the virtual image directly onto the user's retina. In other words, the retina itself provides the screen for the virtual image, which will be as detailed as any computer graphics produced on a monitor.[13]

Psychological Effects

Mental health professionals have expressed concern about the psychological impact virtual reality may have on users, who experience a loss of contact with the real world. Some individuals may be especially at risk, including drug users, individuals with schizophrenia or other mental disorders, and people who are emotionally unstable.[14]

However, due to the recent emergence of virtual reality technology, little research exists to support psychologists' health concerns.[15] As more individuals and organizations use virtual reality, researchers can study its potentially negative effects. In the mean time, law enforcement agencies should be aware that virtual reality users may experience some ill effects.

CONCLUSION

At present, many individuals equate virtual reality with science fiction; yet, with numerous commercial firms and nonprofit organizations dedicated to its development, virtual reality soon will be an important part of life, especially for law enforcement personnel. By understanding how the technology works and what it can accomplish, law enforcement organizations can become active in research and development and request that applications be developed to meet their special needs.

Virtual reality by no means represents a panacea for all aspects of

police work. However, this new and intriguing technology holds great potential for opening the door to a multitude of possibilities.

In its present form, virtual reality allows law enforcement officers to enter a virtual training environment and react to real-world situations without the accompanying dangers. Virtual environments can be created and re-created to test and evaluate strategies both before and after using them in a real situation.

In the case of the officer in the opening virtual reality scenario, he became caught up in the heat of the moment and entered a dangerous situation without backup. Fortunately, this officer could return to the real world, review his actions, and learn from his mistakes.

Law enforcement officers who make errors in judgment sometimes pay for it with their lives. Virtual reality forgives mistakes and gives officers a second chance.✦

Endnotes

[1] Myrna Marofski, "Training the MTV Generation," *Training and Development Journal*, 9-10.

[2] Ibid.

[3] Carmen Miller, "Online Interviews Dr. Thomas A. Furness, III, Virtual Reality Pioneer," *Online*, November 1992, 14.

[4] Glen Emery, "The Radical Visions of Artificial Reality, *The Washington Times*, May 6, 1991.

[5] Dr. Robert E. Roberts, vice president for research, the Institute for Defense Analyses, interview by author, November 23, 1994.

[6] Ibid.

[7] Ibid.

[8] Tor Berg, "Virtual Reality Resource Guide," *Virtual Reality Special Report*, Fall 1994, 39.

[9] George Grein, supervisor, Emergency Vehicle Operations Center, Los Angeles County Sheriff's Office, Los Angeles, California, interview by author, December 6, 1994.

[10] "Virtual Reality Gets Real," *The Economist*, February 20, 1993, 61.

[11] Clarence Barrett, Human Interface Technology Laboratory, Washington Technology Center, University of Washington, Seattle, Washington, interview by author.

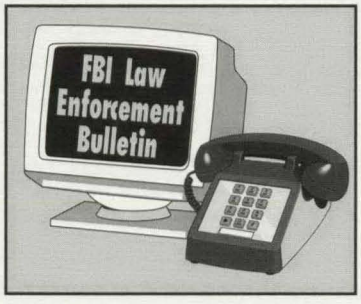
[12] Ibid.

[13] Ibid.

[14] Glenn F. Cartwright, untitled article, *World Future Society*, 1994, 104.

[15] Ibid.

Dial Law Enforcement



Law Enforcement is available via three computer dial-up services. Anyone who has a personal computer and a modem can access, download, or print current issues of *Law Enforcement* in their homes or offices by contacting these services. Those interested in obtaining information regarding these services should dial the following numbers directly:

- SEARCH Group, Inc.
  (916) 392-4640
- IACP NET
  1-800-227-9640
- CompuServe
  1-800-848-8199
  (Ask for Representative 346.)✦

1995 Teleconferences

Imagine sitting in a room, looking at a television monitor, and hearing law enforcement trainers thousands of miles away discuss media relations in a crisis situation, the latest Supreme Court decisions of particular importance to law enforcement managers and officers, or employee assistance programs. Also imagine being able to interact with these trainers, either to ask a question or to make a comment.

Satellite teleconferencing allows law enforcement professionals of all ranks and positions to do just that. It has emerged as one of the most effective training tools available because it offers a viable means of instantaneously communicating up-to-date information in a uniform manner.

The Law Enforcement Satellite Training Network (LESTN), produced by the FBI, broadcasts video teleconferences to law enforcement agencies nationwide. The programs featured on LESTN are intended for all levels of law enforcement personnel and cover a wide array of law enforcement topics.

Broadcasts can be received in any location in Canada, Puerto Rico, and the United States, including Alaska and Hawaii. Each teleconference lasts 2 hours, from noon to 2:00 p.m. Daylight Savings Time, and includes telephone calls and faxes from the viewing audience. The programs, which feature representatives from the law enforcement community, are presented at no cost to agencies and can be videotaped for use in future training sessions.

Agencies can receive broadcasts if they have a C-Band dish antenna, a television monitor, and a tuner. Or, they can use a facility that has satellite receiver equipment, such as an emergency services center, hospital, college or university, etc. An information flier sent to all law enforcement agencies lists the schedule and satellite coordinates for each broadcast.

The LESTN teleconference broadcast in April 1995 covered police media relations in crisis situations. This program addressed pre-crisis planning, the role of the department's spokesperson, interagency coordination, managing the media at the scene, and post-event actions. The topics and dates for the remaining two teleconferences scheduled for 1995 are *Legal Update 1995* on July 26 and *Employee Assistance Programs* on September 13.

Satellite teleconferencing provides a valuable service, because with this form of communication, educators reach a wide audience scattered in various locations thousands of miles apart. And, as every officer knows, better communications and more training mean better service to citizens and to the law enforcement profession. ✦

Video copies of aired teleconferences can be obtained by submitting a written request on department letterhead to SA Tom Christenberry, the LESTN Program Manager, FBI Academy, Quantico, VA 22135. The fax number is 1-703-640-1673.

By Invitation Only
Managing the Annual Street Party

By Ronald R. Thrasher, M.S.

Many communities stage annual celebrations. They may rally motorcycles, harvest peaches, kick off a rodeo, or remember a moment in history. These events can bring communities together or set the stage for tragedy. A celebration that the public perceives as an economic boon literally may be a bust. In fact, only the police may understand the true cost of managing large, often-intoxicated crowds.

This article explores the local "street party," contrasting community perceptions and forces that drive such events with actual observations. This information may provide police with ways to manage street parties and other major events by helping to change public opinion about their costs and benefits to the community.

THE STILLWATER CELEBRATION

In July 1987, a local restaurant started a new tradition in Stillwater. It promoted its anniversary with a weekend party, which became an instant success. In addition to attracting families, the event also drew crowds of college students from nearby Oklahoma State University.

Over the years, the party grew quite popular and soon became a week-long celebration. Local merchants were pleased with the event; they viewed it as a family-oriented reunion that brought the town increased revenues. But, Stillwater police were about to change that perception.

How Much Revenue Does It Generate?

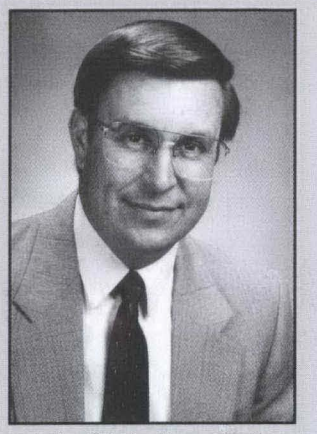
To estimate the amount of revenue the party generated for the city, an Oklahoma State University professor surveyed visitors to the annual Stillwater celebration by distributing questionnaires at motels, restaurants, and retail stores. The survey showed that the average visitor in town for the day spent $100; the average overnight visitor, $130, for each day of what was, at

the time, a 2-day event. Given crowd estimates, the chamber of commerce, the visitor's bureau, and businesses then advertised that the event annually generated $6.8 million for the local economy.

Stillwater police saw more than dollar signs, however. They saw a predominately college-aged crowd that, according to arrest records, traveled from out of town only to attend the party. Once there, they usually became highly intoxicated. Many of the party-goers arrived just prior to the event and brought their own beer, liquor, and food. Most participants either spent the night with friends, in vacant lots, or in city parks. For the most part, they did not spend money in the community.

An opportunity to patronize the local shops did come when the revelers ran out of beer. Unfortunately, they often cost business owners more money than they spent. One convenience store had to close because the clerks could not control the shoplifting and vandalism. Even in the face of this evidence, many residents still believed that the party provided a major source of revenue for the community.

> ***"Just as criminal investigators profile rapists, murderers, or burglars, police administrators should profile major events that occur within their jurisdictions."***



Lieutenant Thrasher commands the Criminal Investigations Unit of the Stillwater, Oklahoma, Police Department.

How Much Does It Cost?

Police calculated the cost of the event in terms of both time and money. In 1987, a crowd of 10,000 gathered in and around the establishment that organized the party. Police worked 130 hours of overtime, received 89 additional related calls for service, and filed 21 criminal charges. By 1993, the party had grown to a week-long event, with a crowd of over 64,000 people taking up two square blocks. This time, police worked over 3,000 hours of overtime, and in the last 3 days of the party, filed 172 criminal charges. They responded to numerous additional calls for service from parties and disturbances all over the community, which most likely were a result of the street party.

The cost to the police department represented only one area of consideration. Other city agencies provided services during the event, such as supporting officers who worked in 100-degree temperatures, manning remote booking facilities, and providing prisoner transport and night court. City officials also spent time planning and managing the event. Finally, both police and city officials faced potential liability costs in controlling a large, intoxicated crowd.

MANAGING THE EVENT

Changing Public Perceptions

Stillwater police recognized that they could not control the event without changing the public's perception of it. Citizens and promoters who actually attended the celebration often left before party guests got carried away, sometimes literally. The department took photographs and produced a video that illustrated what the others missed—damage, injury, and criminal behavior. In addition to distributing this evidence to the media, the department addressed business and community groups on one of their favorite topics—money.

The police graphed local sales tax revenues for the months of June, July, and August, from 1986 through 1993. Because merchants collect sales tax on all goods and services, these revenues paint a realistic portrait of money spent in the community.

The graph dramatically demonstrated that collected sales taxes had changed little after 1987, the year the party began. In fact, sales tax revenues in August—when Oklahoma State students returned for classes—were substantially higher than in June or in July, when the annual party took place.

In the face of overwhelming evidence, the community realized that the cost of their annual party gave them little reason to celebrate.

Business owners began to work more closely with police and eventually paid for a portion of the overtime required to control the event.

Gathering Information

Over the years, as the police searched for ways to manage the party, they turned to a variety of resources in addition to local business owners. They contacted the police in neighboring communities for suggestions, studied the advertising used in previous years, and critiqued their own procedures. Finally, they gathered essential information just prior to the actual event.

Several weeks before the party, police interviewed convenience store employees, bartenders, bouncers, and anyone who might have heard people mention attending the party. They also contacted local motel managers to elicit information about guests who had reserved rooms for the celebration.

After learning where the individuals resided, officers contacted these cities. They obtained information concerning crime trends, juvenile crime, and gang activity, in the hopes of anticipating and preventing situations they might encounter in Stillwater.

This method was based on the presumption that a majority of the party attendees actually stayed in motels. The police had not discovered yet that few, if any, of the college-aged crowd made such sleeping arrangements. In the long run, the information gleaned from this approach was of little use.

The most valuable information came from behavioral research that plainclothes police officers conducted in drinking establishments. As police watched the drinking habits of patrons both inside and outside, it became apparent that people behaved differently when they drank inside than when they drank on the street or sidewalk.

People inside drank less. They talked, danced, ate, and played video games. Many small arguments resolved themselves when one individual walked away. When interviewed, these patrons indicated that they wanted to take the fight outside because the manager would either throw them out or call the police. Managers said that they were eager to report disturbances to the police to protect their businesses and their liquor licenses.

> ***"A celebration that the public perceives as an economic boon literally may be a bust."***

Outside, the scenario changed considerably. People drinking on the street or sidewalk appeared to have little to do but drink. They seemed to consume more alcohol and become more intoxicated. Fights that occurred on the street quickly turned into brawls.

The street also became the "in" place to hang out for young people under 21, the legal drinking age. Their overheard conversations often concerned some type of criminal activity. Gang recruitment and even drug sales occurred within these groups. When questioned, participants said the chances of getting caught doing something wrong were much less outside. There, they had a better chance of escaping.

Laying Down the Law

To curb illegal activity, police considered implementing a local law banning public beer consumption.[1] A prior law had proved successful but short-lived. Enacted in 1978, it was repealed in 1982, primarily due to the efforts of university students, who lobbied persistently, then turned up in record numbers to vote. From 1978 to 1982, Part I offenses[2] dropped 18 percent from the 4 years before the ordinance took effect. Four years following the law's repeal, Part I offenses increased 29 percent.

Two other college towns with similar laws had experienced an 8.13-percent decrease and a 15.79-percent decrease in Part I offenses after prohibiting public beer consumption. Of five other Oklahoma cities with public consumption laws, four experienced decreases of 12 percent, 10 percent, 6 percent, and 21 percent. Only one experienced a 5-percent increase, similar to the statewide crime trend at the time.

Using this information, police helped support a ban on public beer consumption. Voters enacted a local ordinance a few months prior to the 1994 street party.

Businesses also responded by advertising a month-long event rather than highlighting the street party. Publicity for the event emphasized a family-oriented reunion and did not mention drinking. Posted signs announced the ban on public consumption.

Seeing Results

Although the celebration took place as planned, the street party did not. Business establishments confined the festivities to their own properties; crowds did not spill onto the streets. Attendance fell to fewer than 1,000 people the weekend of the traditional street party, with families representing the majority of the guests. On Saturday night—typically the evening of heaviest activity—police made no related arrests. They also reported almost total voluntary compliance with the public consumption law.

Finally, from a business perspective, sales tax revenues for that month *increased* almost $60,000 from the previous year. These profits reflected the increased number of families and other individuals who spent more time and money inside local businesses and at other tourist attractions, instead of crowds of youths who did little more than party in the street.

CONCLUSION

Just as criminal investigators profile rapists, murderers, or burglars, police administrators should profile major events that occur within their jurisdictions. Factors to consider include the type of event; who or what drives the event; who attends the event and why; what costs and profits are realized and who incurs them; and what is required to change the nature of the event. Then, the police should bring their concerns to the community and work to enact a solution, which may involve changing public opinion.

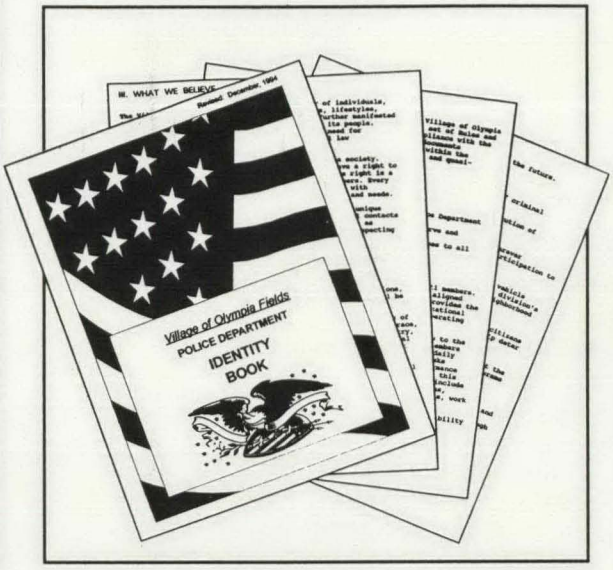
Annual celebrations often put police between the threat of tragedy and the perception of large local revenues. By profiling these events, police may discover that the foundations are fragile and easy to dismantle. The time to control the party is not while the beer bottles are flying and the trash dumpsters are burning, but well before the invitations go out.✦

Endnotes

[1] State and local law has prohibited the public consumption of liquor since 1986. By State law, liquor and beer are defined and regulated separately.

[2] The FBI Uniform Crime Report defines Part I offenses as criminal homicide, forcible rape, robbery, aggravated assault, burglary, larceny, motor vehicle theft, and arson. Arson was not included in this study.

Police Practice



Developing an Identity Book

By Mark Fazzini, M.S.

During the past several years, many law enforcement agencies have adopted progressive management styles, overhauled departmental policies, and updated mission statements to reflect a more community-oriented approach to policing. Intradepartmental documents and policy manuals have been revised to reflect the important changes taking place in police agencies across America. However, despite all of the updating and revising, departments rarely consider tying all the facets of structure, mission, and policy together in a single document that projects a clear picture of their organization.

The Olympia Fields, Illinois, Police Department decided to create such a document. The *Olympia Fields Police Department Identity Book* draws from various sources, such as policy manuals, employee handbooks, and current ordinances, to present a clear image of the department's structure and functions in a single document.[1] The department's identity book also gives readers, whether they are residents, politicians, or police recruits, an understanding of something often difficult to glean from policy manuals—the agency's ideological identity.

What is an Identity Book?

An identity book defines a department's unique mission, philosophy, strategic goals, organizational makeup, and decisionmaking processes. Its primary purpose is to combine elements from various existing documents to give readers a more comprehensive image of the organization.

Deciding to Develop an Identity Book

When the idea of developing an identity book was initially discussed, two practical questions arose—"Why is it needed?" and "How will it benefit the department?" An identity book has several uses and can be extremely helpful in a variety of settings. Simply by distributing the document to civic leaders or members of the local news media, an agency can enhance understanding and support for its operations within the community.

However, other uses abound. Police departments can distribute identity books to:

- Homeowners' associations or individual residents to give them a better understanding of the structure, philosophy, and decisionmaking process of the department. Such a document can answer a number of questions often posed by residents who want to learn more about the police department
- Public officials so that they can refer to the identity book as a source of documentation for the police department. In fact, a properly drafted identity book can be used as documentation to help defend against discrimination claims and other legal actions directed at the police department
- Employees, particularly new recruits, to provide them with a clear picture of the organization's structure. Employees who understand better the mission and philosophy of the department can more effectively perform the often-complex tasks required of them.

Because an integral function of the identity book is to foster community support for the police department,

distribution generally should be as broad as the budget allows.

Deciding the Contents

Each department can decide how much information to include in its identity book. The *Olympia Fields Police Department Identity Book* is 10 pages long and is divided into 6 chapters that answer fundamental questions about the department.

The first chapter, "Who We Are," provides a brief history of the department, its current staffing level, and operations. The next chapter, "What is Our Purpose," incorporates a formal mission statement and the six-fold program of services provided by the department. These include:

1) Creating a safe atmosphere throughout the Village of Olympia Fields

2) Promoting the philosophy of community policing

3) Responding to all service calls and treating all individuals with dignity and respect for their individual rights

4) Upholding—both publicly and privately—the highest standards of the law enforcement profession

5) Improving the ability of officers to perform their tasks through continual training, and

6) Fostering an environment for officers to continue their education for self-improvement.

The third chapter, "What We Believe," is dedicated to a statement of affirmative equal opportunity. It is followed by an explanation of the police organizational structure in chapter 4, "What Our Structure Is."

The final two chapters, "Where We Are Going" and "How We Make Decisions," are dedicated to the department's strategic goals for the future and its basis for making operational decisions. The last chapter also reports on the department's administrative philosophy.

> **"An identity book defines a department's unique mission, philosophy, strategic goals, organizational makeup, and decisionmaking processes."**

An appendix shows an organizational chart of the police department and its administrative affiliation within the city government. Agencies may choose to include the names of city officials, relevant committees, assignments of all police personnel, or even a community map outlining police beats.

In preparing an identity book, agencies can limit the contents to what they believe is relevant to those who may read the document. Of course, strategic assets must not be compromised, but the book should provide enough information to give readers from outside the department a complete overview of the agency.

A statement of affirmative action and/or equal opportunity should be included in a chapter describing the ideals for which the agency stands. Recognizing individual dignity in a clear statement of nondiscrimination promotes a positive view for everyone who makes judgments about the police department based on what they read in the identity book.

Drafting an Identity Book

The information presented in an identity book may seem simple, but what appears straightforward to a police official may look much more complex to an outsider. Therefore, the more departmentalized an organization, the more detailed the document should be to ensure that readers understand the agency as fully as possible.

Dividing the information into sections on patrol, investigation, and administration may provide an adequate level of detail for small or medium-sized departments. However, the more levels of decisionmaking in an agency, the greater the need to explain the intricacies of the decisionmaking process.

Planners also must ensure that documents referenced in the identity book do not contradict one another. Instead, the individual sources need to support structure and policies in a uniform manner.

Enforcing policies becomes difficult when rules and regulations state one thing while employee policy manuals state another. The process of drafting an identity book can bring all of these various documents into alignment.

Obtaining Employee Input

In creating its identity book, the Olympia Fields Police Department distributed draft copies to each member of the command staff and posted a copy for the patrol staff to review. All members of the department had an opportunity to review the document before the administrative staff solicited suggestions for changes or additions. In doing this, the staff ensured that each employee had an opportunity to provide input in the formulation of the identity book. This increased the likelihood that department personnel would support the final product.

> **"...each agency should review and update its identity book on an annual basis to include the latest information on the department's structure and policy."**

Tying It All Together

To give the identity book credibility, the document should reference appropriate State statutes, city ordinances, and internal regulations that provide the basis for the police department's authority to perform the functions described. Further, by specifying statutes by chapter and section number, the document affords readers the opportunity to confirm specific points of the law or statutory authority vested in the agency.

Administrators also must understand that developing an identity book does not eliminate the need for existing policy manuals or other agency documents. An identity book should complement the other documents by tying them all together. In most cases, existing manuals and documents address topics in greater depth than would an identity book.

Finally, as with other documents, an identity book should evolve as an agency adapts to meet the changing needs of its community. Every law enforcement agency should review and refine policy and procedures continually to serve these changing needs. Accordingly, each agency should review and update its identity book on an annual basis to include the latest information on the department's structure and policy.

Conclusion

The most successful commercial firms devote considerable resources to forging and maintaining a strong individual identity with customers. Progressive law enforcement agencies should take their cue from these successful organizations.

An identity book helps establish a clear image of the police department for a community's residents. It shows how the agency fits within the community to perform the duly-authorized functions established by State statutes and municipal ordinances. It provides the public with insight into a department's internal structure and decisionmaking processes.

The *Olympia Fields Police Department Identity Book* gives readers an indication of the future direction of the police department. By providing this information to citizens, identity books do more than give residents a clearer picture of police structure, functions, and decisionmaking; they also help break down some of the barriers that can separate a community from its police department. ✦

Agencies interested in obtaining a copy of the *Olympia Fields Police Department Identity Book* should submit a request on agency letterhead to Lt. Mark A. Fazzini, Olympia Fields Police Department, 20701 Governors Highway, Olympia Fields, IL 60461.

Lieutenant Fazzini serves with the Olympia Fields, IL, Police Department.

Computer Crime Categories

How Techno-criminals Operate

By DAVID L. CARTER, Ph.D.

> *"The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros—little bits of data—it's all electrons....There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information—what we see and hear, how we work, what we think. It's all about information."*
>
> Lines from the character "Cosmos," in the movie *Sneakers*, MCA/Universal Pictures, 1992.

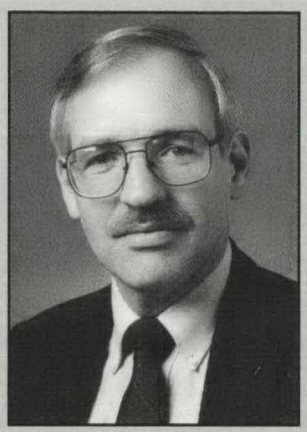
The motion picture *Sneakers* focused on computerized information as a valuable commodity and on the technological means to invade and steal that commodity. To many, the high-tech wizardry of the movie probably appears exotic; however, it is much more realistic than some assume. If there is a lesson to be learned from the movie, it is that the potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes.

Discussions of emerging technological crimes center mostly on computer crime, with the inference that there is only one type of offense. This is not, however, the case, because specific categories of computer crime exist.

As computer-related crimes become more prevalent, an increasing need emerges for police personnel—particularly those who do not have expertise in computer technology—to understand how these crimes vary. An understanding of the types of computer-related crimes will assist law enforcement by providing insight for investigative strategies.

TYPES OF COMPUTER CRIMES

There are primarily four general types of computer crimes. However, in practice, multiple crimes, that is, concurrent criminality or lesser offenses, can occur during any given criminal transaction, resulting in an overlap between the classifications.



> ***"...the potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes."***

Dr. Carter is a professor in the School of Criminal Justice, Michigan State University, East Lansing, Michigan.

Computer As the Target

Crimes in which the computer is the target include such offenses as theft of intellectual property, theft of marketing information (e.g., customer lists, pricing data, or marketing plans), or blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference). These crimes also could entail sabotage of intellectual property, marketing, pricing, or personnel data or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations.

Unlawful access to criminal justice and other government records is another crime that targets the computer directly. This crime covers changing a criminal history; modifying want and warrant information; creating a driver's license, passport, or another document for identification purposes; changing tax records; or gaining access to intelligence files.

Techno-vandalism occurs when unauthorized access to a computer results in damage to files or programs, not so much for profit but for the challenge. In such cases, the damage or loss may be intentional or accidental.

Another crime in this category is techno-trespass, that is, "walking" through a computer just to explore. In such cases, the intruder only looks at a file, but even this violates the owner's privacy. This would be the technological equivalent of a criminal trespass.

In all of these crimes, the offender uses the computer to obtain information or to damage operating programs. The offender commits the crime either by "superzapping" or by becoming a "super user." These labels mean that the offender accesses the operating program by masquerading as the system's manager, thus giving the intruder access to virtually every file in the system.

Not surprisingly, becoming a super user is relatively easy for individuals experienced in computer operations, because virtually every operating system has a trap door that allows individuals to enter a system and declare themselves the system's manager. Trap doors permit access to systems should a problem, either a human or technological one, arise. Unfortunately, this device also poses a threat to the system's integrity.

One of the best examples of a crime in which the computer is the target can be found in the book *The Cuckoo's Egg* by Cliff Stoll. The book recounts the true story of a hacker from Hanover, Germany, who infiltrated a number of computers in the United States, including those of universities, the military, and government contractors. The hacker attempted to locate and steal national security information in order to sell it to foreign governments, a clear illustration of making computers the targets of crime.

Computer As the Instrumentality of the Crime

In common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime. In this category, the processes of the computer, not the contents of computer files, facilitate the crime.

Essentially, the criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime. Another method involves converting legitimate computer processes for illegitimate purposes. Crimes in this category include fraudulent use of automated teller machine (ATM) cards and accounts; theft of money

from accrual, conversion, or transfer accounts; credit card fraud; fraud from computer transactions (stock transfers, sales, or billings); and telecommunications fraud.

One example of using a computer as the instrument to commit a crime is the growing problem of individuals' using cellular phones and electronically billing charges to other customers. In these cases, offenders obtain cellular billing identification codes by using scanning devices, which are small parabolic (curve-shaped) antennae connected to portable computers. When activated, these scanners capture and store account numbers transmitted by cellular phones.

The offenders operate near highways, because motorists frequently make calls from their cars. Once they capture the computerized billing codes, they program these codes into other cellular phones simply by hooking up the phone to a personal computer. Then, using software originally developed by programmers in London, they reprogram the signal chip in the cellular phone. The use of this software, which is easy to copy and to use, is spreading across the United States and Canada, sometimes being shared through underground computer bulletin board services (BBS).

Computer Is Incidental to Other Crimes

In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act. This means that the crime could occur without the technology; however, computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify and trace. Such crimes include money laundering and unlawful banking transactions, BBSs supporting unlawful activity, organized crime records or books, and bookmaking. In one case, a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

Cases involving drug raids, money laundering seizures, and other arrests also have produced computers and electronic storage media containing incriminating information. Many times, the criminals encrypt the data or design the files to erase themselves if not properly accessed. In some instances, criminals even destroy the storage media, such as disks, to eliminate evidence of their illegal activities.

> ***"...the elements of a computer-related offense must be established for successful prosecution...."***

All of these situations require unique data recovery techniques in order to gain access to the evidence. And, in every case, the crimes could occur without the computers; the systems merely facilitate the offenses.

Another illustration of how criminals use technology to further their illegal activities involves child pornography. Historically, consumers of child pornography have trafficked photographs and related information through newsletters and tightly controlled exchange networks. Now, with the advancement of computer technology, child pornographers exchange this information through BBSs.

Recently, U.S. Customs agents raided 40 locations in 15 States serviced by a Denmark-based, child pornography BBS. These criminals used the computer to facilitate the distribution of pornographic material and to increase the efficiency of criminal activity already occurring via other methods.

Crimes Associated With the Prevalence of Computers

The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes. In these cases, technological growth essentially creates new crime targets. Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category of computer crime.

One offense in this category occurs with relative frequency—the violation of copyright restrictions of commercial software. Initially, this offense may not seem like a serious crime; yet, the potential loss to businesses can be quite staggering.

A software package usually costs about $400; a strong-arm robbery usually yields about $50 or less for the thief. Thus, *one* copyright violation is the economic equivalent of *eight* strong-arm

robberies. However, because the emotional trauma experienced in a piracy is almost nonexistent, many people do not view this as a serious crime.

Evidence exists that software also is being written and sold explicitly to help hackers break into computers. In another area, successful computer programs—notably word processing, spreadsheets, and databases—are being duplicated, packaged, and sold illegally on a large scale, just as audio and video tapes are pirated. Similarly, counterfeit computers and peripherals (items such as modems and hard disks) are being manufactured and sold as originals in much the same manner as imitation Rolex watches and Gucci shoes.

PERSPECTIVE ON LEGAL ISSUES

Offenses vary by both the criminal act and the jurisdiction. Some States have enacted laws specifically directed toward crimes involving computers, while other States rely fundamentally on the common law as it applies to current and emerging technology. As with any other crime, the elements of a computer-related offense must be established for successful prosecution, not a particularly easy task in light of the nature of computer technology.

For example, the criminal intent, *mens rea*, of a specific computer crime may be difficult to prove. How does an investigator distinguish between a hacker who intentionally steals or destroys electronic files and someone who accidentally destroys files while simply perusing them? This is definitely not a simple question to answer, and it will continue to perplex investigators, given the nature of changing technologies and the inventiveness of the generally intelligent people who tend to commit computer-related crimes.

Similarly, the physical act of a computer-related crime, *actus reus*, may be demonstrated best by an electronic impulse that, unfortunately, is difficult to define and track, considering that a computer crime can occur in 3 milliseconds using a program code that tells the software to erase itself after the computer executes the action. Essentially, this eliminates the evidentiary trail.

These issues provide similar problems for the criminal element of causation, typically found in statutes relying on the common law. Causation in this regard relates to the self-destruction of computer programs that facilitate "cyber" crimes. How can an investigator show causation if the offender erases the executing instructions?

Additionally, the electronic data interchange (EDI) and its networks complicate the legal elements by making it more difficult for law enforcement to specify, document, and materially link the crime to an individual. The EDI connects parties via computer for contract negotiations, sales, collections, and other business transactions. The computer becomes the vault, with the EDI serving as the key to its contents. The ability to access data in the computer must be relatively easy in order to maximize business efficiency; yet, security controls must be introduced in order to protect the business' "crown jewels."

Unfortunately, maximum security and easy accessibility are not compatible. Consequently, because businesses generally prefer user-friendly equipment, system security usually takes second priority. The phenomenal growth of computer BBSs, on-line services, and the Internet only serves to compound the problem. As a result, computer-related crimes become easier to perpetrate and more difficult to identify, investigate, and prove.

SPECIAL PROBLEMS WITH COMPUTER-RELATED CRIME

Intellectual Property

Discussions of computer-related crime refer with increasing frequency to intellectual property. While the term is familiar to many, its actual meaning may be somewhat elusive.

Intellectual property consists of concepts, ideas, planning documents, designs, formulas, and other information-based materials intended for products or services that have some commercial value or represent original thoughts or theses. Crimes associated with intellectual property focus primarily on theft

when the product has commercial value, as opposed to basic research or research for private use.

In some instances, the theft takes place when a competitor manufactures a similar product developed from stolen intellectual property. In other cases, the crime occurs when the offender mounts countermarketing strategies after learning of a competitor's product through illegal, electronic means, oftentimes referred to as competitive intelligence.

Frequently, these crimes are difficult to discover and even more difficult to prove. The problem becomes further complicated when the property is still in the developmental stages with its final design or application still incomplete.

The investigation and prosecution of thefts of intellectual property with clear protection—such as intellectual property that is copyrighted or has a trademark, patent, or registered trade secret—have more of an advantage than when the protection of such property can be debated. This latter category includes unprotected research and development, original concepts and ideas yet to be realized, and public domain information modified with individual refinements. These areas provide particular challenges for investigating and proving a wrongdoing.

Intellectual property can be divided into two broad categories. The first involves formulas, processes, components, structure, characteristics, and applications of new technologies and covers such areas as fiber optics, computer chip designs and conductivity, and telecommunications equipment, protocols, and technologies, to name a few.

The second category of intellectual property takes in factors associated with the marketing and production of new technologies. Pricing information, marketing targets, product release dates, and production timetables would be included in this category.

> ***"Protocols must be developed for law enforcement that address the various categories of computer crime."***

Malfeasance by Computer

The concept of malfeasance by computer means that computer-related behavior stretches the bounds of legality and may be viewed as only technically wrong, despite its widespread, potentially negative impact. Without question, a variety of computer-related behaviors border on illegality but are not clearly defined as such. Although sometimes done with the best intent, the behavior poses ethical problems, at the very least. The following scenarios illustrate the problem:

- A parent offers to copy a computer program for a school that cannot afford to buy the software
- An employee secretly maintains a small database in an office computer as part of a sideline business
- An individual uses someone else's computer account number and password to view the contents of a database
- A customer gives her unlisted telephone number as part of a sales transaction at a store. The store enters the number into a computerized database and later sells the data to a telemarketing firm without the customer's permission
- A university computer programmer develops a program to schedule classes as part of a job assignment. The programmer then accepts a job with another university and leaves with a copy of the program for use at the new place of employment.

These illustrations point to the "gray" areas of computer abuse—areas that fall increasingly on the shoulders of law enforcement to address and resolve.

International Issues

Americans tend to have a provincial view that the United States is ahead of the rest of the world in many areas, especially technological development. While this is true to some extent, the lead is not as great as many would believe. Japan and Germany, in particular, have shown themselves to be strong technological innovators and consumers. In general, technological knowledge and expertise contribute to the growth of computer-related crime on an international level.

Americans must be concerned about the growth of computer-related crime capabilities emerging outside U.S. borders because of the ease of information exchange and the high concentration of

computer-driven businesses and research projects in the United States. However, it appears that the area of most rapid growth will be in Europe as a result of the treaties signed to create the European Community. Among the important elements of the act that established the basis for unification are open communications, a single, European-wide communication protocol, a strong profit-oriented market spanning 12 countries, open borders, unification of technology standards, and easier banking, including monetary transfers between countries.

While businesses can make great use of these unifying measures, so can criminals. Emerging international crime-related issues most probably will accompany the unification of Europe. These issues include industrial espionage (competitive intelligence), economic/political espionage, expansion of international organized crime beyond traditional areas, and theft of technological hardware.

CONCLUSION

Criminals have adapted the advancements of computer technology to further their own illegal activities. Unfortunately, their actions have far out-paced the ability of police to respond effectively.

Protocols must be developed for law enforcement that address the various categories of computer crime. Investigators must know the materials to search and seize, the electronic evidence to recover, and the chain of custody to maintain. Without question, law enforcement must be better prepared to deal with the many aspects of computer-related crimes and the techno-criminals who commit them. ✦

Bulletin Reports

NCJRS On-line

The National Criminal Justice Reference Service (NCJRS) offers access to criminal justice information through the Internet. The NCJRS gopher menus can connect users to resources of the National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, Office for Victims of Crime, Bureau of Justice Statistics, Bureau of Justice Assistance, and Office of National Drug Control Policy. They also provide direct links to NCJRS*BBS and other criminal justice resources around the world. The gopher address is *ncjrs.aspensys.com71*

Another service offered is NCJRS World Wide Web (WWW), which provides a graphical interface to NCJRS information, as well as to information from other criminal justice resources around the world. The address for the NCJRS WWW is *http://ncjrs.aspensys.com:81/ncjrshome.html*

The Justice Information (JUST INFO) Electronic Newsletter is a free newsletter distributed on the 1st and 15th of every month. To subscribe:

1. **Type** an e-mail to *listproc@aspensys.com*
2. **Leave** the subject line blank
3. **Type** *subscribe justinfo* in the body of the message and then your name (e.g., *subscribe justinfo john doe*)

E-mail also can be used to obtain information and help from NCJRS. First-time users who send an e-mail message to *look@ncjrs.aspensys.com* will receive a reply outlining NCJRS services. For technical assistance or for answers to specific questions on criminal and juvenile justice topics, e-mail should be sent to *askncjrs@aspensys.com*

Partnerships Against Violence Network

PAVNET, the Partnerships Against Violence Network, is a collection of information to assist in building safer, less violent communities. Developed through a coalition of 6 Federal agencies and more than 30 Federal information clearinghouses and resource centers, PAVNET contains information on over 600 antiviolence programs around the Nation oriented toward prevention, enforcement, treatment, or rehabilitation. Also included in PAVNET are 200 information and technical assistance sources that advise where and how to find support for local and State efforts to address issues of violence and 125 funding sources that give details about Federal and private foundation grants.

PAVNET information can be obtained from a printed, two-volume resource guide. Volume 1 (NCJ 150044), *Promising Programs*, contains complete descriptions of all programs, which are indexed by title, subject matter, geographical location, and funding source. Volume 2 (NCJ 150045), *Information Sources, Funding, and Technical Assistance*, has two major sections. The information and technical assistance section identifies sources for direct help and information, including teaching materials. The funding resources section describes the guidelines to obtain funding to address antiviolence projects and contains a list of publications on funding.

PAVNET data also are available on the Internet. Gopher to *pavnet.esusda.gov*; select 6 from the main menu. The *PAVNET Online User's Guide* (NCJ 152057) offers guidelines on how to navigate the PAVNET menus and to search for specific topics and describes various options for traveling the information superhighway to reach PAVNET.

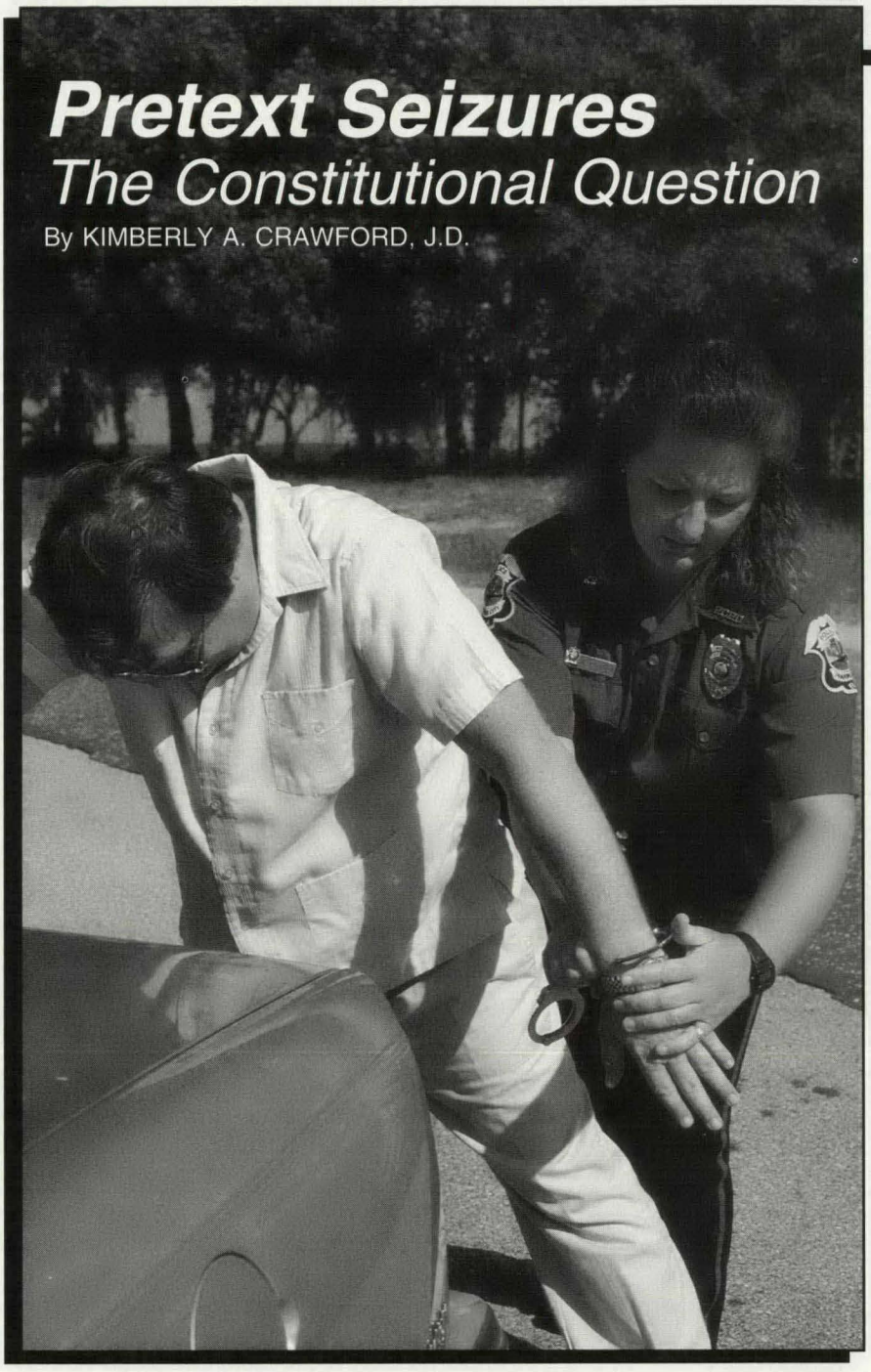
To obtain a copy of any of the guides, call the National Criminal Justice Reference Service (NCJRS) at 1-800-851-3420. Written requests can be sent to NCJRS, PAVNET, Box 6000, Rockville, MD 20849-6000 or faxed to 1-301-251-5212. PAVNET also will be available for a nominal fee on diskette in either WordPerfect 5.1 or ASCII formats.

Civil Remedies for Criminal Behavior

A publication of the National Institute of Justice, *Using Civil Remedies for Criminal Behavior: Rationale, Case Studies, and Constitutional Issues*, reports on seven case studies that illustrate different approaches to using civil remedies to combat crime and diverse illegal behaviors. The case studies show how civil remedies were employed to address crimes involving domestic violence, hate crime, possession of dangerous weapons, car theft rings, and drug dealing in public and private housing. The publication also reports on how to make effective use of civil remedies and how to use civil statutes in a constitutionally defensible manner.

This NIJ publication can be obtained from the National Criminal Justice Reference Service, Box 6000, Rockville, MD 20850. The toll-free number is 1-800-851-3420.

Photo © K.L. Morrison



Pretext Seizures
The Constitutional Question

By KIMBERLY A. CRAWFORD, J.D.

The fourth amendment to the U.S. Constitution prohibits unreasonable searches and seizures.[1] *Searches* are presumed unreasonable if conducted without search warrants and the burden of proof is on the government to establish that a warrantless search was justified under an exception to the warrant requirement.[2]

With respect to *seizures*, there is no presumption that the government needs a warrant. To be reasonable under the fourth amendment, seizures need only be based on governmental interests that outweigh the intrusions upon an individual's privacy rights.[3]

In theory, the formula for determining the reasonableness of a seizure is relatively simple: The greater the intrusion on an individual's privacy interests, the more facts and circumstances the government must have to support its claim of an overriding interest. Thus, an arrest, which is the most significant form of seizure, requires the government to establish its interests to the level of probable cause.[4] In contrast, an investigative detention, which is a much reduced intrusion, requires only a showing of reasonable suspicion.[5]

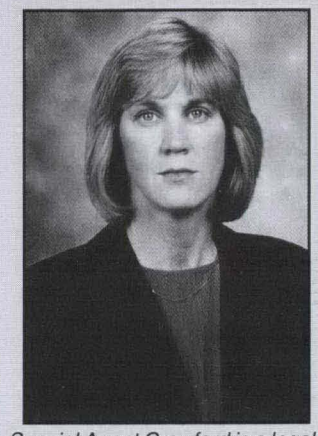
In reality, however, determining the reasonableness of a seizure can be an extremely difficult task. No mathematical or scientific formula exists for predicting when facts and circumstances rise to the level of reasonable suspicion or probable cause; yet, law enforcement officers are required to make such judgments on a daily basis and act on them. Once acted upon, those judgments are subject to seemingly endless defense challenges.

Traditionally, defense challenges to seizures have centered around the facts and circumstances used to justify the action or the amount of force used to accomplish it. However, one defense challenge to seizures goes beyond the traditional arguments and focuses on the law enforcement officer's state of mind. This challenge alleges that a seizure is unconstitutional if the seizing officer has an ulterior motive and uses

the seizure merely as a pretext to allow further investigation.

This article discusses the nature of pretext seizures and reviews the courts' methods for determining their legality. Additionally, it suggests a law enforcement practice to combat defense challenges alleging unlawful pretext seizures.

> ***"...one defense challenge...alleges that a seizure is unconstitutional if the seizing officer...uses the seizure merely as a pretext to allow further investigation."***



Special Agent Crawford is a legal instructor at the FBI Academy.

HISTORICAL BACKGROUND

One of the first cases of note to address the issue of pretext seizures was *State* v. *Blair*.[6] In *Blair*, police officers investigating a murder had as their primary evidence a palm print on the door of the victim's van. An anonymous tip indicated that a member of the Blair family was involved in the crime.

Finding that three of four members of the local Blair family had major case prints on file and that none of the prints matched the one on the victim's van, the police focused their attention on Zola Blair, the fourth member of the family. Although Zola had no prints on file, the police discovered that there was an outstanding traffic warrant for her arrest. After executing that warrant, the police obtained finger and palm prints from Zola and questioned her about the murder before booking her on the traffic warrant and allowing her to make bond.

When fingerprint experts made a match on the prints, the officers arrested Zola on a murder warrant. She then made incriminating statements during interrogation. Prior to trial, however, the defense moved to suppress both the fingerprint evidence and the incriminating statements as being the products of an unlawful pretext arrest. The prosecution, on the other hand, argued that the original arrest of Zola Blair was pursuant to a lawful traffic warrant and that any ulterior motive on the part of the law enforcement officers was irrelevant.

Finding that the defendant had been treated as a murder suspect when arrested and not as a minor traffic offender,[7] the trial court concluded without precedent that the arrest was unlawful because it was pretextual and that the evidence obtained as a result of that arrest were fruits of the poisonous tree. Following an appeal in which the State supreme court upheld the trial court's order of suppression,[8] the U.S. Supreme Court granted certiorari.[9] However, the Supreme Court subsequently dismissed the writ of certiorari as being improvidently granted.[10]

Because the lawfulness of the arrest in *Blair* was the predominant issue in dispute, a Supreme Court decision in the case undoubtedly would have determined the legality of pretext seizures. Unfortunately, the Supreme Court's refusal to hear the case left the legality of pretext seizures unresolved and allowed State and lower Federal courts to reach their own conclusions regarding the lawfulness of such seizures. As a result, the courts' approach to pretext seizures has been inconsistent.

SUBJECTIVE APPROACH

The subjective approach, which apparently was used by the State court in *Blair*, focuses exclusively on the law enforcement officer's state of mind at the time of the seizure. If a seizure on a relatively minor offense is motivated by a law enforcement officer's desire to investigate a more serious offense, the initial seizure is deemed to be a pretext and considered unlawful.

Following *Blair*, the Circuit Court of Appeals for the Ninth Circuit was the only court to adopt temporarily the subjective approach. In *United States* v. *Smith*,[11] the appellate court warned that "an arrest may not be used as a pretext to search for evidence. Whether an arrest is a mere pretext to search

turns on the motivation or primary purpose of the arresting officers."[12] Thus, the court cautioned that an arrest for a minor traffic offense that was motivated by the desire to search the vehicle for evidence of some other unrelated offense for which the police lacked probable cause would be unconstitutional.

Despite this admonition, the Ninth Circuit Court of Appeals subsequently upheld a stop based on probable cause to believe that a driver was operating a vehicle without a license, despite the fact that the police admittedly had an ulterior motive to search the car for drugs. The court's decision in *United States* v. *Cannon*[13] marks a clear departure from its earlier subjective approach to pretext seizures.

The Ninth Circuit's digression from the subjective approach virtually was mandated by a number of Supreme Court decisions.[14] Although repeatedly refusing to address the issue of pretextual seizures specifically,[15] the fourth amendment interpretation espoused by the Supreme Court over the past decade unquestionably demands an objective approach to search and seizure issues.

In *Maryland* v. *Macon*,[16] for example, the Supreme Court emphasized that "[w]hether a Fourth Amendment violation has occurred 'turns on an objective assessment of the officer's actions in light of the facts and circumstances confronting him at the time' and not on the officer's actual state of mind at the time the challenged action was taken."[17] In light of such unequivocal language endorsing an objective standard for review of fourth amendment issues, the subjective approach to pretext seizures is clearly baseless.

OBJECTIVE APPROACH

With the demise of the subjective approach to pretext seizures, it would seem that State and Federal courts would be consistent in adopting an objective standard. To some extent, this is true. Currently, all appellate courts confronted with defense claims of improper pretext seizures purportedly evaluate the government's actions on the basis of objective reasonableness. If the seizure is objectively reasonable, then it is lawful, despite any ulterior motive on the part of the government.

Unfortunately, courts do not always agree on what makes a seizure objectively reasonable. Some courts use a "could have" test, while others use a "would have" test.

"Could Have" Test

When determining the lawfulness of an alleged pretext seizure, courts that apply the "could have" test simply require the government to establish that the seizure was authorized.[18] Any law enforcement officer "could have" made the seizure because there were sufficient facts, amounting to either probable cause or reasonable suspicion, to justify the intrusion.

In *United States* v. *Scopo*,[19] the Court of Appeals for the Second Circuit used the "could have" test to uphold a motor vehicle stop that subsequently led to the seizure of an altered weapon and the prosecution of an organized crime figure for the possession of that weapon. The vehicle in question was being driven by defendant Ralph Scopo, a known member of an organized crime family engaged in an internal "war."

Surveillance teams first observed the vehicle double parked on the wrong side of the road and later make two unsignaled lane changes. After following the vehicle for approximately 2 miles, officers seized the vehicle as it paused for a red light. As the officers approached the vehicle with weapons drawn, they observed the defendant throw something into the back seat. After ordering the defendant out of the vehicle, officers looked into the back seat and found a fully loaded revolver in plain view.

After being charged with the possession of an illegal weapon, defendant successfully moved to have the evidence suppressed on the grounds that the stop of his vehicle for traffic violations was a mere pretext to search his car for weapons. The district court found that the pretext nature of the seizure was evidenced by officers' testimony that traffic stops often were used to confiscate weapons from organized crime figures and that the stop was

made more than 2 miles from the traffic violation.

On review, the Court of Appeals for the Second Circuit reversed the dismissal order. In doing so, the court refused to look beyond whether the officers had probable cause to arrest the defendant for the traffic violation. Instead, the court held that "when an officer observes a traffic offense—however minor—he has probable cause to stop the driver of the vehicle."[20] Reviewing the facts before it, the court noted that the officers had directly observed the defendant violating the traffic laws and, consequently, had probable cause to arrest him.

The "could have" test for determining the legality of a seizure is straightforward and effectively thwarts any defense claim of pretext. Because courts that use the "could have" test focus their attention exclusively on factual justifications, seizures based on probable cause or reasonable suspicion are lawful, regardless of any alleged pretextual motivation.

"Would Have" Test

When confronted with a pretext challenge, courts that apply the "would have" test go beyond the factual justifications for a seizure and determine whether a reasonable law enforcement officer "would have" made the seizure absent an ulterior motive. Accordingly, a seizure based on probable cause or reasonable suspicion may be deemed unconstitutional if a reviewing court determines that under the same circumstances, a reasonable officer would not have made the seizure.

In *United States* v. *Smith*,[21] the Court of Appeals for the 11th Circuit used the "would have" test to conclude that the stop of a weaving vehicle was pretextual. The subsequent search of the vehicle, although based on probable cause, was considered tainted by the unlawful seizure.

> ***"...courts that use the 'could have' test focus their attention exclusively on factual justifications...."***

A Florida Highway Patrol officer assigned to a special drug squad observed the vehicle in *Smith* traveling north on Interstate 95 at 3:00 a.m. The officer testified that he followed the vehicle because he suspected it might be carrying drugs but did not stop it until he observed it weaving and crossing into the emergency lane. After stopping the vehicle, the officer used a drug detection dog to locate 1 kilogram of cocaine in the trunk. The driver was later charged with possession with intent to distribute.

Following his conviction, defendant contested the admissibility of the cocaine on the grounds that it was discovered as a result of a pretext seizure. The government, on the other hand, argued that the weaving of the vehicle gave the officer the reasonable suspicion necessary to investigate the possibility of drunk driving and that any officer under the circumstances could have made the seizure.

Vacating defendant's conviction, the Court of Appeals for the 11th Circuit rejected the "could have" analysis championed by the government and opted to apply the "would have" test. In doing so, the court considered whether a reasonable officer would have stopped a vehicle weaving slightly and crossing the line into the emergency lane without an ulterior motive. Concluding that a reasonable officer would not have made such a stop, the court gave the following explanation:

> That an officer theoretically *could* validly have stopped the car for a possible traffic infraction was not determinative. Similarly immaterial was the actual subjective intent of the [officer]. The stop was unreasonable not because the officer secretly hoped to find evidence of a greater offense, but because it was clear that an officer would have been uninterested in pursuing the lesser offense absent that hope.[22]

Although courts that apply the "would have" test profess to be using a purely objective approach, subjectivity inevitably creeps into the analysis. Courts will not employ the "would have" test unless they believe an officer had a subjective ulterior motive for making the seizure. The ulterior motive does not necessarily invalidate the seizure, but it will cause the courts using the "would have" test to consider what a reasonable officer would have done under the circumstances absent an ulterior motive.

The "would have" test has a substantial disadvantage in that it

requires courts confronted with a pretext challenge to go beyond the particular facts of a case and consider what has been done under similar circumstances in other cases. Courts using this test cannot review the facts of the case before them and simply decide whether the officer had probable cause or reasonable suspicion to make the seizure. Rather, these courts must consider whether and under what circumstances officers made similar stops in the past.

For example, when confronted with a defense challenge that a traffic stop for making an illegal turn was pretextual, a court using the "would have" test cannot simply determine that the officer making the stop had reason to believe the traffic laws were violated. Instead, if the court believes the officer had an ulterior motive when making the stop, it must consider how frequently officers stop drivers for illegal turns when no ulterior motive exists.

COUNTERING THE "WOULD HAVE" TEST

Because a number of State and Federal courts[23] use the "would have" test, law enforcement agencies should be prepared to meet the pretext challenge. They can do so by keeping accurate, detailed records regarding the number and types of seizures made.

For instance, when confronted with the challenge that a traffic stop for an illegal U-turn or an unsignaled lane change was pretextual, a law enforcement agency could refute that challenge by establishing the consistency with which its officers make such stops. In essence, the records serve as testimony that established procedures, not ulterior motives, govern the actions of the officers.

CONCLUSION

Defense claims of pretext have found favor in some State and lower Federal courts. Agencies can prepare to rebut such claims by maintaining detailed records regarding all seizures, especially traffic stops. Unless the Supreme Court resolves the issue of pretext seizures by adopting the "could have" test, these accurate, detailed records may be the governemnt's best defense to claims of pretext. ✦

> ***"Courts will not employ the 'would have' test unless they believe an officer had a subjective ulterior motive for making the seizure."***

Endnotes

[1] U.S. CONST. amend. IV.

[2] *Katz* v. *United States*, 389 U.S. 347 (1967).

[3] *Graham* v. *Conner*, 490 U.S. 386, at 395 (1989).

[4] *Wong Sun* v. *United States*, 371 U.S. 471 (1963).

[5] *Terry* v. *Ohio*, 392 U.S. 1 (1968).

[6] 691 S.W. 2d 259 (Mo. 1985)(en banc).

[7] When they arrested her, officers read Blair her constitutional rights before taking her to the homicide unit, where they booked her on homicide charges. They then took major case prints. She was detained overnight before being released. *Id.* at 262.

[8] *Id.* The case resulted in a 4-3 decision with a very cogent dissent filed by Judge Blackmar.

[9] 106 S.Ct. 787 (1986).

[10] 107 S.Ct. 1596 (1987).

[11] 802 F.2d 1119 (9th Cir. 1986).

[12] *Id.* at 1124 (citations omitted).

[13] 29 F.3d 472 (9th Cir. 1994).

[14] The Ninth Circuit cited *Maryland* v. *Macon*, 472 U.S. 463 (1985), and *Scott* v. *United States*, 436 U.S. 128 (1978).

[15] In one term, the Supreme Court denied certiorari in five cases involving pretext seizures. *See, United States* v. *Trigg, United States* v. *Cummins*, and *United States* v. *Enriquez-Navarez*, 112 S.Ct. 428 (1991); *Anderson* v. *Illinois*, 112 S.Ct. 89 (1991); and *Hope* v. *United States*, 111 S.Ct. 1640 (1991).

[16] 472 U.S. 463 (1985).

[17] *Id.* at 470-71 (quoting *Scott* v. *United States*, 436 U.S. 128 (1978).

[18] *See, United States* v. *Ferguson*, 8 F.3d 385 (6th Cir. 1993) (en banc); *United States* v. *Hassan El*, 5 F.3d 726 (4th Cir. 1993) (petition for cert. filed); *United State* v. *Cummins*, 920 F.2d 498 (8th Cir. 1990) *cert. denied*, 112 S.Ct. 428 (1991); *United States* v. *Trigg*, 878 F.2d 1037 (7th Cir. 1989), *appeal after remand*, 925 F.2d 1064, *cert. denied*, 112 S.Ct. 428 (1991); *United States* v. *Causey*, 834 F.2d 1179 (5th Cir. 1987)(en banc); *United States* v. *Scopo*, 19 F.3d 777 (2d Cir. 1994); *United States* v. *Hawkins*, 811 F.2d 210, *cert. denied*, 108 S.Ct. 110 (1987); *People* v. *King*, 36 Cal. Rptr. 2d 365 (Cal. App. 1995); *State* v. *Lopez*, 873 P.2d 1127 (Utah 1994); *Randle* v. *State*, (unpublished) 1994 WL75807 (Tex. App. 1st Dist.); *State* v. *Bea*, 864 P.2d 854 (Or. 1993); *State* v. *Swanson*, 838 P.2d 1340 (Ariz. 1992); *People* v. *Haney*, 480 NW2d 322 (Mich. App. 1992); and *State* v. *Law*, 769 P.2d 1141 (Idaho Ct. App. 1989).

[19] 19 F.3d 777 (2d Cir. 1994).

[20] *Id.* at 782 (quoting *United States* v. *Cummins*, 920 F.2d 498 (8th Cir. 1992)).

[21] 799 F.2d 704 (11th Cir. 1986).

[22] *Id.* at 710 discussing *United States* v. *Cruz*, 581 F.2d 535 (5th Cir. 1978)(en banc).

[23] *See, United States* v. *Guzman*, 864 F.2d 1512 (10th Cir. 1988); *United States* v. *Smith*, 799 F.2d 704 (11th Cir. 1986); *United States* v. *Cannon*, 29 F.3d 472 (9th Cir. 1994); *People* v. *Owens*, ___ NYS 2d ___ (NY 1995); *State* v. *Chapin*, 879 P.2d 300 (Wash. App. 1994); *State* v. *Turner*, (unpublished) 1994 WL313053 (Ohio App. 2d Dist); *State* v. *Izzo*, 623 A.2d 1277 (Me. 1993); *Robinson* v. *State*, 617 So. 412 (Fla. Ct. App. 1993); *Townsel* v. *State*, 763 P.2d 1353 (Alaska Ct. App. 1988).

Law enforcement officers of other than Federal jurisdiction who are interested in this article should consult their legal advisor. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

The Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. *Law Enforcement* also wants to recognize their exemplary service to the law enforcement profession.

Officer Krebs

While responding to the robbery of a cab driver, Officer Julia Krebs of the Savannah, Georgia, Police Department observed a subject attempting to conceal himself along the riverfront. Upon seeing Officer Krebs, the subject ran and jumped into the Savannah River to elude apprehension. As the man attempted to swim across the wide river, Officer Krebs saw that he had become fatigued and was in danger of drowning. Without regard to potential dangers, including swift river currents, commercial ship traffic, and limited nighttime visibility, she dove into the river and convinced the combative subject—who was drunk and 60-pounds heavier than Officer Krebs—to accept her assistance. She kept the man afloat until both were picked up by a Coast Guard vessel. Officer Krebs both rescued and apprehended an escaping offender.

Trooper Leggett

Trooper John Wayne Leggett of the Mississippi Highway Patrol became suspicious of a sport utility vehicle bearing out-of-state license plates. When he turned to follow the vehicle, the driver sped away as the passenger fired several shotgun rounds at the trooper's vehicle. Although Trooper Leggett's eyes were slightly injured by shattered glass from the windshield, he pursued the speeding vehicle. The chase ended when the suspects crashed their vehicle. After a short gun battle, Trooper Leggett arrested the pair, who had escaped from a North Carolina prison 6 days earlier. They stole the vehicle in Florida and kidnaped its owner, whom they later killed. After their arrest, one of the suspects led investigators to the site in Georgia where they had left the owner's body.

Officer Carr

Officer Pat Carr of the Forest Park, Ohio, Police Department was driving to court when the vehicle in front of him suddenly swerved into an embankment and flipped over, landing upside down in a travel lane of the highway. He positioned his patrol cruiser to protect the scene and was radioing for assistance when he noticed smoke beginning to pour out of the overturned car. The sole occupant was unable to exit the vehicle. Officer Carr forced open the driver's side door to find a woman hanging upside down from her safety belt. He freed her from the burning vehicle and treated her for shock and a leg injury until medics arrived. Officer Carr then helped other motorists to control the blaze using available fire extinguishers.

U.S. Department of Justice
Federal Bureau of Investigation

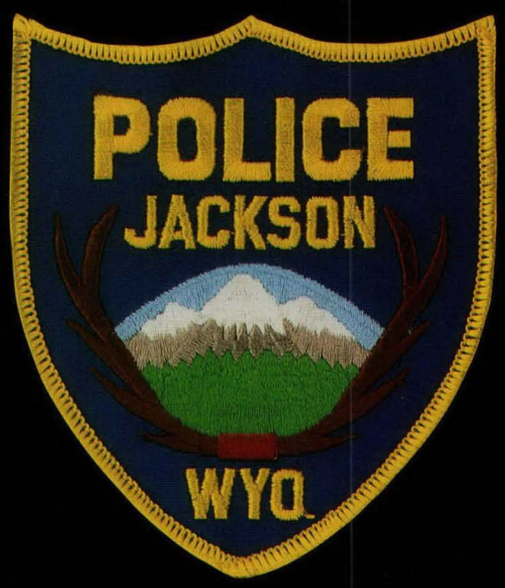
Second Class Mail
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Washington, D.C. 20535

Official Business
Penalty for Private Use $300

Patch Call

The patch of the Bennington, Vermont, Police Department depicts the Bennington Battle Monument and flag. The original Bennington flag was carried by patriots during the Battle of Bennington in 1777 and is preserved in the town's museum.



The Jackson, Wyoming, Police Department patch features the Teton Mountain Range framed by a set of elk antlers. Known as the gateway to both Yellowstone and Grand Teton National Parks, Jackson is located just south of the National Elk Refuge, winter home to nearly 10,000 North American elk.