

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

## Coplink: Database Detective

**I**t's called a "Web-based intuitive integrated interface." But in layman's terms it's called "Coplink." What it will do is help put an end to a serious problem faced by law enforcement every day . . . the inability to exchange information about criminal cases across jurisdictions.

With the help of a nearly \$1 million grant from the National Institute of Justice (NIJ), the Tucson, Arizona, Police Department and the University of Arizona's Artificial Intelligence (AI) Laboratory are making Coplink a reality. When completed, Coplink will be a mechanism that not only links databases, but also searches these databases for associations and links between people, places, and things.

"We're trying to provide a way for law enforcement agencies to share information, specifically case information, and to bring it all together in an integrated system where they can also do some sophisticated types of analysis on the information," says Sgt. Jenny Schroeder, project leader at the Tucson Police Department, where the system is being tested. As a trial, Schroeder's department has integrated its records management system, gangs database, and video mug shot database.

"The problem with having lots of isolated systems is that you have to search multiple records and databases," Schroeder says. "The first hallmark of Coplink

is that it takes legacy data, puts it into a warehouse, and uses a Web-based interface to make the information available to criminal justice agencies. It doesn't imply a change in anyone's operational system, it simply makes data from other agencies available."

Similar initiatives that pool information are typically in the form of a distributed database system, wherein all participants maintain and control their own databases. The Coplink project, however, warehouses and integrates the data at a local or regional level. These local or regional systems can then be interconnected into a large distributed law enforcement "intranet" or a group of "extranets." As technology moves ahead, new applications can be added and the interface improved incrementally. Agencies will not have to undergo redevelopment to take advantage of the rapidly changing technology. As integration with other agencies occurs, users will continue to have the same easy interface, which will keep training costs down.

With Coplink, agencies can use data from other jurisdictions and government entities that is stored on widely differing systems and computer platforms. Jurisdictions will be able to maintain data security, yet efficiently and quickly provide vital information to partner agencies. It is an aggressive approach that requires more work in the early stages but allows agencies to use more sophisticated analysis tools later on, Schroeder says.



Photo by Danny Hart, Aspen Systems Corp.

No tool similar to Coplink has been available previously because the technology that would foster this kind of connectivity and interoperability did not exist. In addition to NIJ's support, the creation of this technology was aided by scientists at the University of Arizona's Artificial Intelligence Laboratory with funding from the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA).

Hsinchun Chen, Ph.D., a University of Arizona professor of management information systems and the AI laboratory director, says an initial \$7 million in NSF and DARPA funding in part paid for the laboratory's creation of a software program that helped the Central Intelligence Agency analyze data and relationships relating to Russian technologies and their use of those technologies. Chen says that when a machine—not a person—extracts the meanings and relationships between data, it is termed "machine learning." This ability to analyze data and relationships is the second hallmark of the Coplink project. Developed at the University of Arizona, Coplink uses "concept

space," a data-mining tool that points out the relationships between objects, whether those objects are

(See Coplink, page 2)



## Hide and Seek

**T**he alert eye of a staff member spotted a suspicious package the morning of January 2,

1997, at the Federal penitentiary in Leavenworth, Kansas. The staffer notified prison authorities, who searched the mailroom and found yet another suspicious envelope. The local bomb squad was immediately contacted and the area evacuated. X-rays of the envelopes revealed that they contained explosive devices. But that was not the end of it. Additional explosive devices similar to those discovered in the prison mailroom were intercepted at the Washington, D.C., office of El Hayat, a Saudi Arabian newspaper, and at the Leavenworth post office. Although no one was hurt in the incident, the Federal Bureau of Prisons (BOP) took the threat very seriously.

Coming in many shapes and sizes, contraband can be life threatening to staff and inmates.

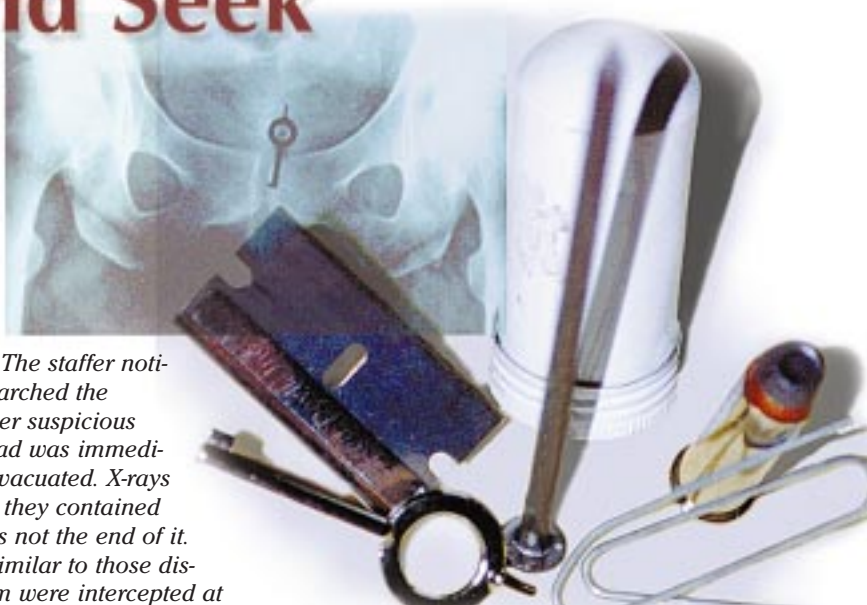


Photo courtesy Ranger Security Detectors, El Paso, Texas.

Its detection is paramount to the safe and orderly operation of every correctional facility. It is for these reasons that the BOP's Office of Security Technology, with funding assistance from the National Institute of Justice, continuously

(See Hide and Seek, page 2)

*Coming Up: NIJ Technology Institute for Corrections*

**October 25-29, 1999**      **Washington, D.C.**



**Mission:**  
To promote effective and affordable technology in support of corrections.

**Agenda/Goals:**

Provides participants the opportunity for continued education on existing and developing technologies related to the corrections field and for problemsolving through technology implementation and lessons learned. Also provides the National Institute Justice (NIJ) the opportunity to enhance its programs through participant feedback, comments, and recommendations. Includes briefings at NIJ's Office of Science and Technology and a local correctional institution.

**Registration:**

Limited to 25 middle-level corrections practitioners who regularly deal with technology issues in their departments or agencies. Contact Jeri Allen, National Law Enforcement and Corrections Technology Center-National, at 800-248-2742 for an application or for additional information.

*(Coplink . . . cont. from page 1)*

people, vehicles, organizations, locations, weapons, or crimes.

In a preliminary test case, the Tucson police agreed to help a Federal agency track down a homicide suspect, even though the agency did not know the suspect's name. The agency had only a confidential informant's tip that the suspect had a sister living in Tucson who several years ago had been assaulted by her boyfriend. The agency did have the boyfriend's name from the complaint, which the Tucson police ran through concept space. In less than a minute, the system returned the woman's name and the name of her brother.

The Coplink project is expected to yield a proof-of-concept prototype for both the database interface and concept space. "Everything will be very simple," Chen says. "Users won't have to memorize function keys. It will work just like the Web: point and click."

After further development and testing, Schroeder says, the plan is to link the Tucson department with the Phoenix Police Department and

later to extend the project to agencies throughout the State. The near-term project goal is to share public record case information with other agencies. However, current Coplink users hope to resolve issues of legality and coordination to share more investigative and intelligence information.

When fully developed, Coplink users hope to see it made available either commercially or through a nonprofit foundation created specifically to package and sell it. "We want to see it made available at a reasonable cost," says Tom Coty, NIJ project manager. "The public paid for its development with tax dollars, and we want to be sure it's readily available and affordable for the users."

**For more information about Coplink, contact Tom Coty at the National Institute of Justice, 202-514-7683; Sgt. Jenny Schroeder at the Tucson Police Department, 520-791-4499; or Dr. Hsinchun Chen at the University of Arizona, 520-621-4153**

*(Hide and Seek . . . cont. from page 1)*

researches and evaluates devices that can aid prison staff in the detection of contraband during their daily activities.

Because of the Leavenworth and *El Hayat* letter bomb incidents, BOP began considering mail screening technologies that could complement its existing mail x-ray procedures, according to Karen Hogsten, acting director of BOP's Office of Security Technology. In its research, she says, her office came across the SCANMAIL 10K, a device manufactured in England and used extensively overseas and in Canada. The device was in the process of being introduced and marketed in the United States.

SCANMAIL is not an x-ray device and does not detect explosives. Instead, it finds metal objects in letters, magazines, padded mailers, newspapers, paperback books, and catalogs. The scanner provides visual and audio alarms when metal is detected, while ignoring normal office items like staples and paper clips.

BOP tested the device at the Metropolitan Corrections Center in New York City. Nine test pieces were concealed among inmate and staff mail, including a blank .22-caliber bullet; a utility knife



razor blade; a 3-inch piece of a hacksaw blade; a handcuff key; a penny; a small 1.5 volt battery (like those used in electronic greeting cards); a blank 9 mm bullet; a small, gold, foil-lined computer chip; and an electronic greeting card with wires and a battery.

According to Hogsten, "SCANMAIL did not miss a thing." Every test piece was detected in every mail item. Mail items that were too thick for the 2.25-inch opening, such as a phone book, were simply opened, laid face-down lengthwise, then fed through the scanner. Letters were put through four and five at a time with the test pieces contained in the middle letter. The test pieces were detected with 100-percent accuracy, as was a padded mailer with five magazines with the test pieces in the middle magazine, and a padded mailer with three paperback books inside. BOP officials conducted additional tests, in which metallic objects were concealed in clothes, shampoo bottles, baby powder, and soap bars.

Staff members in the prison's mailroom noted that using SCANMAIL did not significantly increase their processing time for screen mail. They also recognized that while the device is not a substitute for normal x-ray procedures, it can complement standard mailroom security tools such as x-rays and canines.

Hogsten says that in addition to mail screening devices, BOP was interested in identifying a technology that would provide immediate, reliable, nonintrusive, and noncontact screening of inmates for small weapons and/or metallic contraband that can be concealed in body cavities. The most commonly used methods involve metal detection devices and visual searches. X-rays are the most effective means for searching body cavities; however, they are normally not used for routine processing of inmates.

During its research, she says, BOP investigated the Body Orifice Security Scanner (BOSS). This newly developed metal detector chair incorporates nonmotion static detection and has two independent sensors: one mounted in the seat for rectal and vaginal region detection and a second, countertop sensor mounted on the side of the chair for oral region detection. When an inmate sits in the chair or places his or her chin on the oral scanner, audio and visual alarms alert the staff if there is a metallic object located in the scanned orifice.

*Photo courtesy Ranger Security Detectors, El Paso, Texas.*

The detectors are sensitive enough to detect a handcuff key 6 inches from the sensor surface.

In researching the BOSS chair, BOP discovered that the New York City Department of Corrections had used it with good results. Based on this information, BOP put BOSS chairs in four of its facilities for 90-day evaluations. During that time, the devices detected two contraband items that were not discovered by handheld metal detectors—a razor blade and a gold chain with a medallion. Both items were wrapped in tape, placed in the cut-off finger of a rubber glove, and concealed in the inmate's rectum. Also, shrapnel and dental work that went undetected by metal detectors and were not visible through normal visual search procedures were detected by BOSS and later verified through medical and dental x-ray records. According to Hogsten, BOP staff indicated much more confidence in conducting visual searches after using the BOSS chair than without the use of the chair. Both SCANMAIL and the BOSS chair have been installed in numerous Federal facilities.

"These are just two examples of available products or their equivalent that meet or exceed BOP specifications," Hogsten says. "Other products may also be available that meet or exceed these specifications. Presently BOP also is investigating the use of digital closed-circuit television and passive alcohol detection sensors."

**For more information on any of these technologies, call the Federal Bureau of Prisons' Office of Security Technology at 202-307-3191.**



*Photo courtesy Scanna MSC Inc.*

# Where Users Aren't Losers

Are you a "user?"

You should be.

These days, not being a user—a user of the Internet that is—can certainly be a major disadvantage to law enforcement and corrections agencies.

To keep law enforcement and corrections personnel from falling behind the Internet curve, the National Law Enforcement and Corrections Technology Center (NLECTC)—Rocky Mountain offers as a free service to criminal justice practitioners a class titled "Internet Resources for Criminal Justice," which teaches how to make the most of the Internet.

"The Internet is a tremendous resource that more and more people are taking advantage of," says Joe Russo, Corrections Specialist for NLECTC—Rocky Mountain and a class instructor. "To illustrate this point, consider the incredible growth in the number of Internet users. In 1997, there were 50 million users worldwide. By the year 2000 it is estimated that there will be more than 100 million users. As they say, 100 million people can't be wrong. These folks have learned that the Internet is an indispensable tool to gather and share information across the entire globe . . . and do it in real time."

According to Russo, the class begins with a brief history of the development of the Internet to provide a perspective on its creation and its evolution over the years. Next, he demonstrates the process for tracking down information. This includes an introduction to a variety of "search engines," along with the logic that goes into structuring a query. Through a series of exercises, students begin to learn which search engines are most effective in specific situations. Russo notes that students are given ample time to practice searching techniques on their own so they understand how these techniques work and become more efficient in their use.

An additional component of the class involves a "tour" of several criminal justice agencies' World Wide Web sites. The goal here, Russo says, is to illustrate the many ways agencies use the Internet to dispense and solicit information. Web sites featured include the California Highway Patrol, where an individual can scan incident report information as it occurs. Photographs of "most wanted" delinquent parents are displayed on the Los Angeles County District Attorney's Office Web site. The New York City Police Department's Web site asks for the public's help in finding missing persons and identifying suspects. Other Web sites provide the capability to search for inmates being held in Illinois Department of Correction facilities, or to search the San Diego County Sheriff's booking log, or to search for registered sex offenders, by precinct, in Chicago.

"But we don't just end the class there," says Mike McGee, Law Enforcement Specialist for NLECTC—Rocky Mountain and another of the class's instructors. "Students are also introduced to the variety of Internet tools and resources useful in conducting investigations, including online calculators to assist in traffic accident investigations, crime scene evidence collection, crime mapping, missing persons searches, explosives information, fraud and scams, unsolved crimes, and many, many others."

As one example, McGee demonstrates for each class a CD-ROM of hate groups that have Web sites on the Internet. Developed by the Simon Wiesenthal Center, this CD provides information on, and Web site addresses for, more than 600 hate groups that use the Internet to recruit young people.

The class concludes with a review of Internet resources for doing research on criminal justice issues. A vast amount of statistics and research studies can be found on the Internet, McGee says, and all you need to do is click a button to download the data you are looking for. Students are shown how to access crime statistics online from such sources as the Federal Bureau of Investigation, the

Drug Enforcement Administration, and a number of individual States. Other important resources include the National Institute of Justice, Bureau of Justice Statistics, National Archive of Criminal Justice Data, and National Criminal Justice Reference Service.

To date, Russo says, the "Internet Resources for Criminal Justice" class has been presented to more than 100 criminal justice practitioners. Classes are held quarterly at NLECTC—Rocky Mountain's host facility, the University of Denver. Agencies interested in the class but unable to travel to Denver can host the training at their facilities. During the past year, the class has been presented onsite to members of the New York City Department of Probation, the New Mexico Gang Task Force, and the Fulton County (Georgia) District Attorney's Office. A computer laboratory with Internet access, such as might be available at a high school or college, is necessary to host the class. There is no cost for instructor time and travel.

For those who cannot come to Denver or host a class, a diskette with the bookmarked Web sites used in the class presentation is available at no charge. This disk, "Criminal Justice Resources on the Internet," contains access to almost 400 sites in a well-organized descriptive format that can be easily downloaded to the Internet browser of a personal computer.

**For additional information about the class, "Internet Resources for Criminal Justice," or to request the "Criminal Justice Resources on the Internet" diskette, contact Joe Russo or Mike McGee at the National Law Enforcement and Corrections Technology Center—Rocky Mountain, 800-416-8086.**



## From the Director

Law enforcement, courts, and corrections officials and officers working in the field know how crucial technology is to their day-to-day operations. In some circumstances, having the right tool can even mean the difference between life and death.

The technological revolution that has swept society as a whole in recent years has also affected the criminal justice system. Some technologies that not long ago seemed advanced—vests that can stop bullets and electronic monitoring of probationers—today seem commonplace. But the revolution continues apace, with ever more spectacular advances now being made, or in the testing stages, or on the drawing board.

As the research arm of the U.S. Department of Justice, the National Institute of Justice (NIJ) has, since its founding 30 years ago, been in the forefront in sponsoring the development, testing, and demonstration of technology to improve the justice system. The development of DNA testing standards, soft body armor, and improved fingerprint evidence collection are some of the many areas in which NIJ has played a leading role.

More recently, with strong support from the Administration and the Congress, NIJ has accelerated the pace of its efforts. Less-lethal technologies to minimize the use of force, computerized mapping to pinpoint and analyze crime patterns, concealed weapons detection to prevent violence, methods of stopping fleeing vehicles to apprehend suspects, and improvements in DNA laboratories to aid in evidence testing—all these capabilities, and others, are now being explored by NIJ. Their application can mean even greater transformations in law enforcement operations.

TechBeat plays an important role as an essential link communicating the latest information about these developing technologies from the National Law Enforcement and Corrections Technology Center. By keeping law enforcement, courts, and corrections personnel current about the tools they can use, the newsletter makes a difference in controlling crime and ensuring justice.

Jeremy Travis  
Director  
National Institute of Justice

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #96-MU-MU-K011 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

# Product Alert!



## Physical Analysis of DKL LifeGuard™ Device

The National Institute of Justice (NIJ) tasked and funded the Sandia National Laboratories (SNL) to conduct a detailed physical analysis, based on fundamental scientific principles, of a DielectroKinetic Laboratories, LLC (DKL), Model 3 LifeGuard™ device to determine if it could function as advertised. The DKL LifeGuard™ devices are marketed as a human presence detector and tracker. The results of SNL's analysis conclusively demonstrate that the LifeGuard™ Model 3 device cannot possibly function as a passive long-range detector of human heartbeats based on the scientific principles of dielectrophoresis.

A summary of Sandia's findings indicates that the passive circuit, attributed to detecting heartbeats based on dielectrophoresis, is actually a nonfunctioning, open circuit. Additionally, this circuit includes a component composed of human hair glued between two small pieces of polystyrene. There was also no discernible feedback mechanism or drive to move the antenna located at the front of the device that would cause it to point toward a beating human heart.

**This analysis summary is provided for informational purposes. A copy of SNL's report titled Physical Examination of the DKL LifeGuard™ Model 3 can be located at [www.nlectc.org/pdf/files/dkllanalysis.pdf](http://www.nlectc.org/pdf/files/dkllanalysis.pdf). For additional information, contact Thomas Coty, National Institute of Justice, at [coty@ojp.usdoj.gov](mailto:coty@ojp.usdoj.gov).**

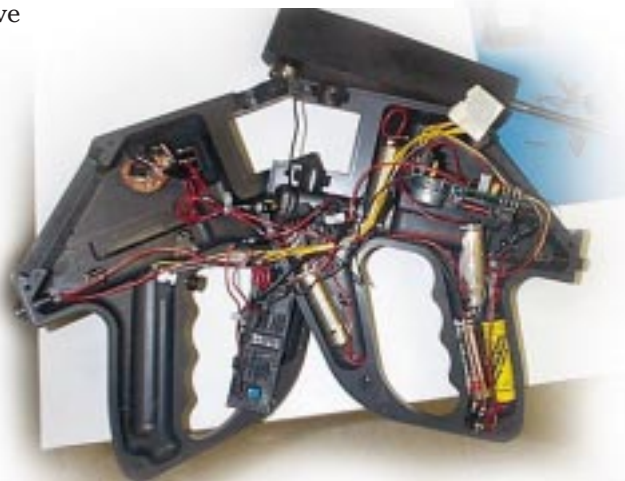


Photo courtesy Sandia National Laboratories.

## Enough To Go Around

If your agency qualifies, everyone in your department or division can now have his or her own copy of *TechBeat* at no cost.

All you have to do is to provide us with the quantity you need and a shipping address (no post office boxes, please). Then as soon as each issue is printed, your agency's copies will be mailed to your attention . . . free. Your only obligation is to disseminate them once they arrive.

**To start this service with our next issue, Fall 1999, contact Rick Neimiller, NLECTC-National, at 800-248-2742 or [rneimiller@nlectc.org](mailto:rneimiller@nlectc.org) by August 31, 1999. Orders after this date will be fulfilled with the Winter 2000 edition. And remember, you can always access TechBeat online at [www.nlectc.org](http://www.nlectc.org).**

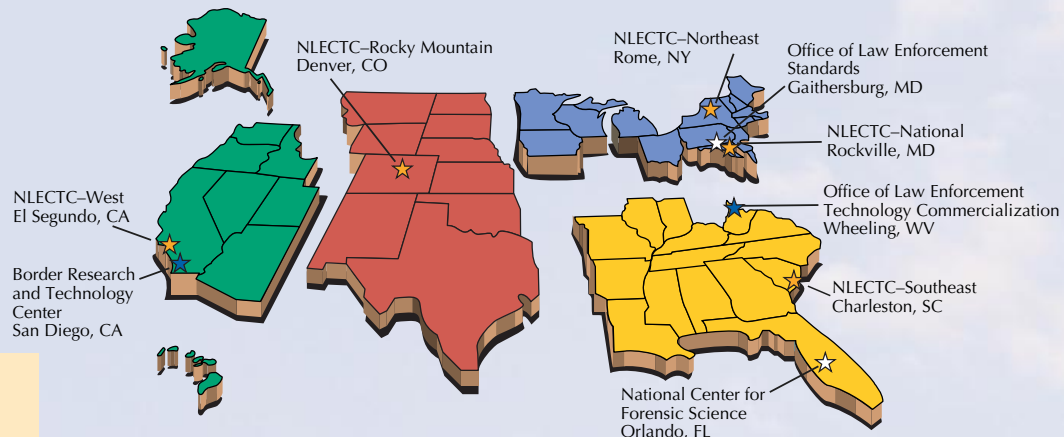
Photo by Danny Hart, Aspen Systems Corp.



# We Got You Covered

The National Institute of Justice (NIJ), responding to recommendations by the law enforcement and corrections community, converted its Technology Assessment Program Information Center (TAPIC) into the National Law Enforcement and Corrections Technology Center (NLECTC) system. Created in 1994 as a component of NIJ's Office of Science and Technology, NLECTC's goal, like that of NIJ, is to offer support, research findings, and technological expertise to help State and local law enforcement and corrections personnel do their jobs more safely and efficiently.

NIJ's NLECTC system consists of facilities located across the country that are colocated with an organization or agency that specializes in one or more specific areas of research and development. Although each NLECTC facility has a different technology focus, they work together to form a seamless web of support, technology development, and information.



## NLECTC-National

2277 Research Boulevard • Rockville, MD 20850

Phone: 800-248-2742 • Fax: 301-519-5149 • E-mail: asknlectc@nlectc.org

The National Center, located just 30 minutes north of Washington, D.C., is the hub of the NLECTC system. It provides information and referral services to anyone with a question about law enforcement and corrections equipment or technology. Its staff manages the voluntary equipment standards and testing program that tests and verifies the performance of body armor, metallic handcuffs, shotguns, and police vehicles and tires. This office produces consumer product lists of equipment that meets a specific set of performance standards and also operates JUSTNET (Justice Technology Information Network), an Internet World Wide Web site that provides links to the entire NLECTC system and other appropriate sites, as well as assistance to those seeking information about equipment, technology, or research findings.

## NLECTC-Northeast

26 Electronic Parkway • Rome, NY 13441

Phone: 888-338-0584 • Fax: 315-330-4315 • E-mail: nlectc\_ne@rl.af.mil

NLECTC-Northeast is located at the Air Force Research Laboratory, Rome Research Site (formerly Rome Laboratory), on the grounds of the Griffiss Business and Technology Park. The center sponsors research and development efforts into technologies that address command, control, communications, computers, and intelligence. This center draws on the expertise of Air Force scientists and engineers in its development of technologies that can be used to detect weapons concealed on individuals, an effort that is expected to yield stationary equipment for use in buildings and handheld devices for field and patrol officers. Other areas of research and development include through-the-wall sensors, audio processing, image processing, timeline analysis, computer forensics, secure communications, and command/control.

## NLECTC-Southeast

5300 International Boulevard • North Charleston, SC 29418

Phone: 800-292-4385 • Fax: 843-760-4611 • E-mail: nlectc-se@nlectc-se.org

Two of the focus areas of NLECTC-Southeast are corrections technologies and surplus property acquisition and distribution for law enforcement and corrections. The center facilitates the acquisition and redistribution of Federal surplus/excess property to State and local law enforcement and corrections agencies. The equipment must be used for law enforcement purposes only. Utilizing the JUSTNET Web site, the center educates law enforcement and corrections professionals about Federal surplus and purchasing programs. The efforts of NLECTC-Southeast have resulted in agencies receiving equipment they would not ordinarily have access to or might not have been able to afford due to budgetary constraints. This facility also studies the needs of corrections agencies. It is guided in this mission by a committee of criminal justice, law enforcement, and corrections practitioners that identifies requirements and sets priorities for research and development. NLECTC-Southeast is allied with the South Carolina Research Authority (SCRA) and the Naval Command, Control and Ocean Surveillance Center In-Service Engineering, East Coast Division (NISE East). NLECTC-Southeast's other areas of focus include information management and technologies, simulation training, and designated special projects.

## NLECTC-Rocky Mountain

2050 East Iliff Avenue • Denver, CO 80208

Phone: 800-416-8086 or 303-871-2522 in the Denver area • Fax: 303-871-2500 • E-mail: nlectc@du.edu

Located at the University of Denver, NLECTC-Rocky Mountain focuses on communications interoperability and the difficulties that often occur when different agencies and jurisdictions try to communicate with one another. This facility works with law enforcement agencies, private industry, and national organizations to implement projects that will identify and field test new technologies to help solve the problem of interoperability. NLECTC-Rocky Mountain also houses the newly created Crime Mapping Technology Center, the training and practical application arm of NIJ's Crime Mapping Research Center, which is staffed by NIJ social scientists and scholars who utilize crime analysis research to improve police field operations and develop crime-mapping software for small, medium, and large departments. The Rocky Mountain facility also conducts research into ballistics and weapons technology, as well as information systems. Sandia National Laboratory has been designated as a satellite of NLECTC-Rocky Mountain. The laboratory works in partnership with NLECTC-Rocky Mountain and focuses on technology for detecting and neutralizing explosive devices (Operation Albuquerque).

## NLECTC-West

c/o The Aerospace Corporation • 2350 East El Segundo Boulevard • El Segundo, CA 90245-4691

Phone: 888-548-1618 • Fax: 310-336-2227 • E-mail: nlectc@law-west.org

NLECTC-West is housed on the grounds of The Aerospace Corporation, a nonprofit corporation that provides technical oversight and engineering expertise to the Air Force and the U.S. Government on space technology and space security systems. NLECTC-West

draws on The Aerospace Corporation's depth of knowledge and scientific expertise to offer law enforcement and corrections the ability to analyze and enhance audio, video, and photographic evidence. In cooperation with The Aerospace Corporation, this NLECTC facility also has available an extensive array of analytic instrumentation to aid in criminal investigations, such as a scanning electron microscope, an x-ray microscope, and a mass spectrometer, all of which are used to process trace evidence. Its other areas of expertise include computer architecture, data processing, communications systems, and identifying technologies to stop fleeing vehicles.

## Border Research and Technology Center (BRTC)

225 Broadway, Suite 740 • San Diego, CA 92101

Phone: 888-656-BRTC (2782) • Fax: 888-660-BRTC (2782) • E-mail: brtchr@aol.com

The Border Research and Technology Center works with the Immigration and Naturalization Service, the U.S. Border Patrol, the U.S. Customs Service, the Office of National Drug Control Policy, and the U.S. Attorney for the Southern District of California to develop strategies and technologies that will facilitate control of the Southwest border. One of its most recognized accomplishments has been the implementation of SENTRI (Secured Electronic Network for Travelers' Rapid Inspection). BRTC also works on joint ventures to identify technologies that will stop fleeing vehicles and is currently participating in a project to detect the heartbeats of people concealed in vehicles or other containers.

## Office of Law Enforcement Standards (OLES)

100 Bureau Drive, Stop 8102 • Gaithersburg, MD 20899-8102

Phone: 301-975-2757 • Fax: 301-948-0978 • E-mail: oles@nist.gov

Supported by NIJ, the Office of Law Enforcement Standards applies science and technology to the needs of the criminal justice community. While its major objective is to develop minimum performance standards for equipment and technology, which NIJ promulgates as voluntary national standards, OLES also undertakes studies leading to the publication of technical reports and user guides. Its areas of research include clothing, communications systems, emergency equipment, investigative aids, protective equipment, security systems, vehicles, and weapons. It also develops measurement methods for analytical techniques and standard reference materials for forensic scientists and crime labs. Since the program began in 1971, OLES has coordinated the development of nearly 200 standards, user guides, and advisory reports. Housed at the National Institute of Standards and Technology, OLES works closely with NLECTC-National to conduct tests and to guarantee the performance and quality of equipment used by police and corrections.

## Office of Law Enforcement Technology Commercialization (OLETC)

Wheeling Jesuit University • 316 Washington Avenue • Wheeling, WV 26003

Phone: 888-306-5382 • Fax: 304-243-2131 • E-mail: oletc@nttc.edu

The Office of Law Enforcement Technology Commercialization, a program of NIJ, is located at Wheeling Jesuit University. OLETC's mission is to work with industry, manufacturers, and laboratories to facilitate the commercialization of technologies for the law enforcement and corrections marketplace. OLETC provides special services and assistance to innovators, entrepreneurs, universities, Federal and other laboratories, and U.S. manufacturers nationwide in commercializing technologies that will enhance the effectiveness of law enforcement and corrections practitioners. A national partnership is being developed to provide a continual pipeline of innovative products, concepts, and value-added services that will expedite the commercialization of new products and services needed for State and local law enforcement and corrections communities. OLETC has directly assisted in commercializing several innovative products, including the RoadSpoke™, a novel vehicle-stopping device; Tiger Vision®, a special low-cost, handheld night vision device; an Explosive Ordnance Disposal Technician Training Kit; and the Counterpoint Stab and Slash Protective Vest. OLETC has identified more than 70 additional emerging technologies and concepts that are currently being evaluated for possible commercialization.

## National Center for Forensic Science

University of Central Florida • P.O. Box 162367 • Orlando, FL 32816-2367

Phone: 407-823-6469 • Fax: 407-823-3162 • E-mail: natlctr@pegasus.cc.ucf.edu

The newest addition to the NLECTC system, this facility is housed in the University of Central Florida and initially will focus on arson and explosives research. Its mission is to conduct fundamental research into the basic nature of fire and explosion reactions, provide the support to develop standard protocols for analyzing arson and explosion debris, promote the use of electronic media to access and exchange information about the forensic sciences, and provide educational opportunities to practicing professionals and full-time students. This new facility will draw on the experience and expertise of the university, which houses a forensic science program with an active research program, as well as the Institute of Simulation and Training, which is currently exploring ways to simulate explosive reactions to study various chemical processes.

# From the Street . . . to the Street

**T**he National Institute of Justice (NIJ) has long believed that one of the most vital aspects of its program is the solicitation of ideas and suggestions from criminal justice practitioners. It is this information that helps form the framework of NIJ's work. NIJ's Office of Science and Technology and its National Law Enforcement and Corrections Technology Center (NLECTC) system acquire this information through conferences, regional workshops, and most especially through a series of advisory groups. These groups are composed of representatives from all areas of law enforcement, corrections, and the forensic sciences, and focus on everything from operational technological needs to liability issues and public acceptance of these new technologies.

One such group, the Law Enforcement and Corrections Technology Advisory Council (LECTAC), is composed of law enforcement, corrections, and forensics practitioners who serve as advisers to the NLECTC system and recommend technology program priorities. Because LECTAC's members are also the end users of new technologies, they bring the day-to-day needs of police and corrections officers to the forefront. As a result of their recommendations, NIJ is able to bring in researchers, scientists, and engineers to address the emerging needs of the law enforcement and corrections communities.

LECTAC's current research priorities include the development of technologies and research in the areas of concealed weapons and contraband detection, vehicle stopping, enhanced DNA testing, officer protection, less-than-lethal technology, information management, counterterrorism, location and tracking, secure communications, and noninvasive drug detection. Following are updates on several sample projects that fall under these headings, many having both law enforcement and corrections applications.

◆ **UPDATE: Sticky Shocker.** The Sticky Shocker is a less-than-lethal projectile that uses stun gun technology to temporarily incapacitate a person at standoff range. The Sticky Shocker is a low-impact, wireless projectile fired from compressed gas or powder launchers and is accurate to a range of 10 meters, sticking to the target with a glue-like substance or with short, clothing-attachment barbs. The projectile incorporates a battery pack and associated electronics that impart a short burst of high-voltage pulses capable of penetrating several layers of clothing. The pulse characteristics are safe, similar to well-established, nonlethal electrical shock devices, and will disable individuals or cause extreme discomfort. Applicable missions include any standoff encounter in which an individual needs to be temporarily incapacitated without exposing law enforcement and corrections officers to unnecessary risk. **Prototype development is complete and has been successfully fired at targets 30 feet**

**away. A safety assessment leading to field trials is under consideration.** For more information, contact David Fields, Joint Program Steering Group, 703-696-2355; or Sandy Newett, National Institute of Justice, 202-616-1471.

- ◆ **Forensic Investigations Information Management System (FIIMS).** The objective of this effort is to develop a way to implement the application of technologies that will enhance the role of forensic science in the criminal justice system. FIIMS includes real-time video, audio, and infrared imagery transmission from a crime scene; telecommunications for distance learning (such as for conducting autopsies); capabilities for case review; image processing and analysis tools; multimedia databases; and the ability to link multiple laboratories throughout the State of New York and the rest of the United States by video conferencing. A technology transfer model has been developed to accelerate the project, which partners NLECTC-Northeast, the Air Force Research Laboratory (AFRL), AFRL's Information Directorate, the New York State Police Forensic Information Center, the New York State District Attorneys Association, and the New York State Division of Criminal Justice Services. For more information, contact NLECTC-Northeast, 888-338-0584.
- ◆ **Video Image Stabilization and Registration (VISAR).** The Video Image Stabilization and Registration project is aimed at taking the "shake" out of shooting video. Arsev H. Eraslan, chief scientist at the Office of Law Enforcement Technology Commercialization, and scientist Paul Meyer have developed VISAR, a new image stabilizing software that uses an imaging algorithm to eliminate shaking, adjust for inadvertent zoom, and brighten dark areas. The software package can highlight an object in an image and line up the pixels from several video frames to produce a steadier, clearer video. It will be patented by scientists at the National Aeronautics and Space Administration's Marshall Space Flight Center. For more information, call Arsev Eraslan at the Office of Law Enforcement Technology Commercialization, 888-306-5382.
- ◆ **Unification of Ballistics Imaging Systems.** The Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology (NIST) has found a way to unify the computerized systems used by law enforcement for ballistics matching. Both the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco and Firearms (ATF) use computerized systems to compare digitized pictures of unique scratches and imperfections on fired bullets or spent

cartridges to similar images housed in an extensive computer database. Matches link bullets or cartridges to a specific gun, providing leads that may help identify criminals. However, the FBI's Drug-Fire and the system supported by the ATF, called IBIS (for Integrated Ballistics Identification System), are not compatible. Among the problems: different lighting used to photograph forensic samples and different mathematical algorithms used to analyze images. The Office of Law Enforcement Standards within NIST's Electronics and Electrical Engineering Laboratory (EEEL) has bridged the gap by addressing the major obstacle separating the two systems. EEEL/OLES specified how the IBIS and Drug-Fire manufacturers could include the other's photographic lighting as an option. Now an IBIS setup can produce data that can be assessed by a Drug-Fire counterpart, and vice versa. With this accomplishment in hand, EEEL/OLES is finalizing a standard to address the dual-system capability and will complete tests later this year to ensure interoperability. For more information, contact Bruce Field at NIST/EEEL, 301-975-4230.

- ◆ **Assessment of State and Local Law Enforcement Needs for Combating Electronic Crime.** NIJ is collaborating with the National Cybercrime Training Partnership (NCTP) to perform a comprehensive needs assessment of State and local law enforcement needs for combating electronic crime. This needs assessment effort is based on a 1998 Summary Report prepared by NCTP's Information Technology Working Group, which recommended that a comprehensive study be conducted to determine State and local law enforcement needs to counter electronic crime. Utilizing its NLECTC system, NIJ launched the needs assessment at a grassroots level. More than 130 State and local criminal justice professionals, representing all 50 States, met in a series of small workshops to identify their current and anticipated future needs in combating electronic crime. A panel of electronic crime experts will be called upon to formulate meaningful conclusions from the information gathered from the criminal justice professionals. These experts will come from industry, academia, and various government agencies. NIJ will produce a final report that will include the following: a summary of the needs expressed by the State and local criminal justice professionals, the conclusions drawn by the panel of electronic crime experts, and recommended technology and point-of-contact resources for addressing the electronic crimefighting needs identified. NIJ anticipates the report will be published in April 2000. For more information about this project, contact Amon Young at NIJ, 202-514-4338.

# The LEO Link



**U**ntil the arrival of the Internet, there was no practical way for law enforcement officers to easily communicate among themselves. Although national networks such as the National Crime Information Center and the National Law Enforcement Teletype System offer access to local, State, and Federal databases, no system has served the needs of the individual officer or law enforcement manager. But with the advent of the Law Enforcement Online (LEO) intranet, law enforcement personnel—right down to the officer level—now have the ability to communicate in a secure mode with one another.

On July 13, 1995, the Federal Bureau of Investigation (FBI) entered into a cooperative agreement with Louisiana State University (LSU) at Baton Rouge to establish the Center for Advanced Support of Technology for Law Enforcement (CASTLE). The center was tasked to be an advanced technological resource to further the state of the art in law enforcement communications capabilities, technologies, and procedures. An initial component of CASTLE has been the creation of LEO.

According to Harlin R. McEwen, FBI Deputy Assistant Director, Criminal Justice Information Services Division, LEO provides a communications mechanism to link all levels of law enforcement in all parts of the United States, supporting broad, immediate dissemination of information concerning the best technologies and practices in law enforcement. LEO is intended to be a user-friendly, no-cost-to-user service, which can be accessed by the law enforcement community using industry-standard personal computers. Exclusively for the law enforcement and criminal justice communities, LEO's unique value, McEwen says, lies in its ability to deliver communications services and distance learning to local, State, and Federal law enforcement on an anytime, anywhere basis. Although still in its early stages, he says, LEO is already becoming an important tool in equipping officers to counter crimes that involve a coordinated effort across United States law enforcement operations.

Currently, LEO provides facilities for electronic communications, including electronic mail (e-mail), chat rooms (private, onscreen interactive keyboard conversations), bulletin boards, Law Enforcement Special Interest Group (LESIG) communications,

and calendars of events. In addition, LEO offers an online library of law enforcement publications, including newsletters, studies, research papers, technical bulletins, and reports of interest to the law enforcement community. Such communications and information are provided to users in a secure user environment. Multiple tiers of security are provided, so that groups with a specialized area of interest may exchange sensitive but unclassified information without concern that it will be compromised or distributed to the broader user community.

A distance-learning capability also has been added to LEO. This capability provides online training courses and material in the latest investigative and enforcement techniques, augmenting the formal training courses offered at the FBI Training Academy at Quantico, Virginia, as well as the training courses offered by other law enforcement agencies. McEwen says that during 1999, LEO is expanding its distance-learning courses by offering training in a larger number of topics. Distance learning, he says, will offer departments a 24-hour-a-day, self-paced education system, which could translate into a significant savings in training costs for a department and allow it to offer more training programs to a greater number of officers.

Also set for expansion during 1999 is the Topical Electronic Library, which is planned to be the repository of a broad range of law enforcement multimedia information available to the vast majority of the law enforcement community. This library will offer timely, secure, and accurate access to information not otherwise available to local, State, and Federal law enforcement.

According to McEwen, any approved employee of a duly constituted local, State, or Federal law

enforcement agency or an approved member of an authorized LESIG can currently access LEO at no cost. At present, users access the LEO system through a national, toll-free, dial-up network, but the addition of other communications delivery systems, such as the Internet, are being considered for the future. LEO currently serves more than 14,000 registered users and is projected to grow to 18,000 users by the end of 1999 and 30,000 users by the end of 2000.

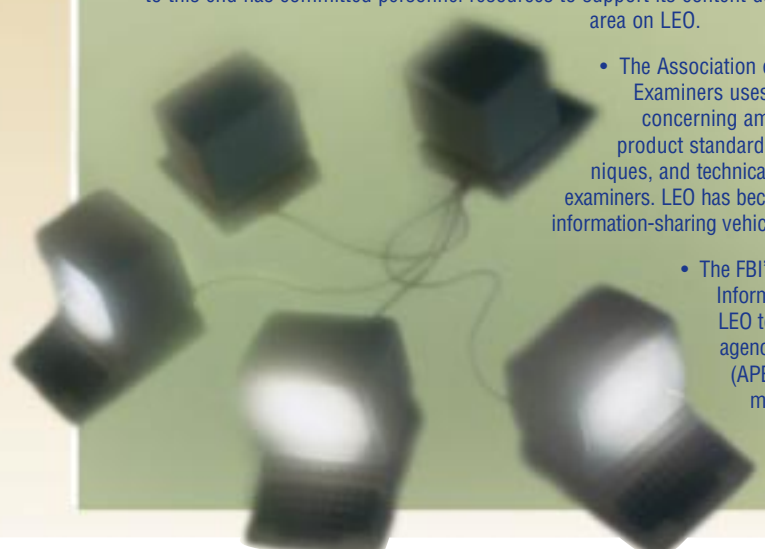
**To go online with LEO, contact the FBI's LEO Program Office, 202-324-8833, and ask for an application, or contact Gary L. Gardner, LEO unit chief and program director, at [ggardner@leo.gov](mailto:ggardner@leo.gov) for more information.**

**Editor's note: In addition to serving as a Deputy Assistant Director for the FBI, Harlin R. McEwen is vice chair of the Law Enforcement and Corrections Technology Advisory Council, which serves as an advisory body to the National Law Enforcement and Corrections Technology Center system.**

*Article art courtesy LEO.*

Since LEO became an operational reality in 1996, many people in the law enforcement community have come to rely on it for secure communication and information sharing, a capability not currently otherwise available. Some examples of participation in LEO include:

- In 1997, the National Sheriffs' Association Executive Board voted unanimously to adopt LEO as its main form of electronic communication with its member sheriffs throughout the United States, and to this end has committed personnel resources to support its content development and manage its area on LEO.
  - The Association of Firearm and Toolmark Examiners uses LEO to share information concerning ammunition, commercial product standards, weapons, forensic techniques, and technical case assistance from other examiners. LEO has become an indispensable information-sharing vehicle.
  - The FBI's Criminal Justice Information Services group uses LEO to communicate with the agency's Advisory Policy Board (APB) and its various subcommittees, exchanging information and receiving feedback
- in a timely and cost-effective manner. This provides significant cost savings over travel and mailing.
- The National Executive Institute (NEI), Law Enforcement Executive Development Association (LEEDA), and Major Cities Chiefs (MCC) are using LEO to facilitate timely communications between members. It is anticipated that this capability will grow into an essential vehicle for peer support and growth in dealing with critical crime and law enforcement administrative problems.
  - The FBI National Academy Associates was one of the initial supporters of LEO, has adopted it as its primary form of electronic communication with its members, and is becoming ever more dependent upon it to facilitate communication and training.
  - LEO is rapidly becoming the main method of contact with and between the FBI Bomb Data Center, FBI special agent bomb technicians, and State and municipal technicians. It is anticipated that by the end of 1999, all bomb squads throughout the United States will be communicating via LEO and relying on it for lifesaving information. LEO has become critical to the exchange of potentially lifesaving information about explosive devices and render-safe tools. Without this capability the realistic potential for loss of life is present. No other forum currently exists or is planned that provides instantaneous information in multimedia form to bomb technicians in life-threatening situations.
  - The FBI Awareness of National Security Issues and Response and the National Infrastructure Protection Center programs use LEO to disseminate time-critical information regarding security issues to law enforcement throughout the Nation as well as the commercial/private sector. This initiative is in direct support of the President's directives on the Critical Infrastructure Protection and Economic Espionage.



# Sign Up To Receive

## Sign Up To Receive Free Reports From the National Criminal Justice Reference Service

In addition to funding the National Law Enforcement and Corrections Technology Center, NIJ also supports the National Criminal Justice Reference Service (NCJRS), an international clearinghouse on crime and justice information. NCJRS staff respond to reference questions, provide referrals to other resources, distribute NIJ and other Office of Justice Programs (OJP) documents, and maintain a mailing list of more than 45,000 registered users. In addition, NCJRS sponsors the *NIJ Criminal Justice Conference Calendar* at <http://www.ncjrs.org/calendar>, which lists conferences and meetings of interest to the criminal justice community. If you are interested in signing up for the NCJRS mailing list, you may request a registration form using any of the following methods:

**Fax-on-Demand.** Dial 800-851-3420, select option 1, then option 2. The registration form is #1 on the document index. The form will be faxed to you immediately.

**Fax.** You may fax your request for a registration form to 410-792-4358. You will receive a form promptly in the mail.

**E-mail.** Send an e-mail to [askncjrs@ncjrs.org](mailto:askncjrs@ncjrs.org) and request a registration form. It will be sent to you in the mail.


**Write.** Send a written request to NCJRS, Box 6000, Rockville, MD 20849-6000.


**Call.** You may call an NCJRS information specialist and request a registration form. The number is 800-851-3420.


As a registered user, you will receive the bimonthly *NCJRS Catalog*, the quarterly *NIJ Journal*, and selected reports based on your criminal justice interests. For more information about NIJ and NCJRS, visit their Web sites: <http://www.ojp.usdoj.gov/nij> and <http://www.ncjrs.org>.


## New Publications/Videos


The following publications/videos are available from the National Law Enforcement and Corrections Technology Center-National:


 **TechBeat, Spring 1999.** This issue of *TechBeat* features the use of surveillance cameras to combat crime, plans to convert an old prison into a training facility for public safety personnel, and preparing computer systems for Y2K compliance.

 **TechBeat, Winter 1999.** Articles in this issue of *TechBeat* discuss the electronic monitoring of inmates in the community, a computer system that allows law enforcement agencies in five States to share information on gang activity, and the Massachusetts State Police program to curb aggressive and dangerous driving.

 **Autoloading Pistols for Police Officers: NIJ Standard-0112.03.** This standard establishes performance requirements and test methods for pistols to be used by law enforcement officers. It is a general revision of and supersedes NIJ Standard-0112.02 dated January 1995, and addresses new pistol designs, calibers, revised procedures for verifying head space, and general revision of the testing procedures.

 **Selection and Application Guide to Police Body Armor.** While body armor is a household word in the law enforcement community, questions about its selection and use are frequently asked. This guide responds to commonly expressed concerns and provides information to help determine the level of protection required by officers.


 **Addendum to NLECTC Publications List.** This supplement lists all publications produced by the NLECTC system since May 1997. The original *NLECTC Publications List* is included with the addendum. Publications are classified in both documents according to the following categories: protective apparel/equipment; weapons/munitions; handcuffs/restraining devices; security systems/equipment; surveillance systems; forensics/criminalistics; communications; vehicles/vehicle equipment; and miscellaneous.


 **"Why Can't We Talk?" When Lives Are at Stake.** This videotape examines the issues and problems surrounding interoperability and public safety radio communications. Learn why planning, designing, and funding public safety wireless communications systems are critical activities for ensuring the public welfare.

 **Land Transportation Security Technology: An Improved Response for a Changing Threat.** This video explores applying technology to improve responses to biological, chemical, and explosive incidents and to threats to transportation systems. Three scenarios are portrayed involving a subway, a train, and a bus. This video should be useful to first responders—police, fire, EMS, and emergency preparedness personnel—and to transportation employees. The video was funded by the National Institute of Justice/Joint Program Steering Group and produced by Oak Ridge National Laboratory and the National Law Enforcement and Corrections Technology Center-Southeast.


The following publications/videos will be available soon:


 **Keeping Track of Electronic Monitoring.** This bulletin will give an in-depth look at current and upcoming home monitoring devices, system components, buy/lease factors and options, and recommendations for establishing an electronic monitoring program.


 **A Comprehensive Evaluation of 1999 Patrol Vehicle Tires.** This bulletin summarizes results of the National Institute of Justice's comprehensive evaluation of patrol vehicle tires, conducted in April 1999.

 **1999 Mock Prison Riot Video.** This videotape features technologies used to quell a mock prison riot staged by the National Institute of Justice's Office of Law Enforcement Technology Commercialization. Emerging technologies were incorporated into training scenarios to demonstrate the latest crimefighting technologies.

To obtain any of the above publications or videotapes or to receive additional copies of the *TechBeat* newsletter, write NLECTC, P.O. Box 1160, Rockville, MD 20849-1160; telephone 800-248-2742. Publications can also be downloaded from JUSTNET at <http://www.nlectc.org>.

 = Online

 = Printed

 = Video



**ONLINE!**  
Body Armor Database—  
a comprehensive listing of all  
models of armor tested and found to  
comply with NJ Standard-0101.03.

- Information
- Publications
- Calendar of Events
- Breaking News
- Services/Assistance
- Technology Projects
- Grants
- Topic Boards
- In the News

**www.nlectc.org**

## NLECTC Is Online

- ◆ **INFORMATION** on new technologies, equipment, and other products and services available to law enforcement, corrections, and the criminal justice communities, including access to a database of more than 4,000 available products and technologies.
- ◆ **ONLINE NEWS SUMMARY** includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major national newspapers, magazines, and periodicals and on national and international wire services and Web sites.
- ◆ **PUBLICATIONS** from NIJ and NLECTC that you can view or download to your system.
- ◆ **INTERACTIVE TOPIC BOARDS** that allow you to post questions and exchange information with hundreds of professionals in their specialty areas.
- ◆ **FREQUENTLY ASKED QUESTIONS** that offer detailed information based on thousands of calls to our information specialists.
- ◆ **CALENDAR OF EVENTS** that lists the latest upcoming meetings, seminars, and training.
- ◆ **LINKS** to other important law enforcement and corrections Web sites.

For help in establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800-248-2742.

Publication images copyright © 1999 PhotoDisc, Inc., unless otherwise indicated.

## Wanted: Good Photos

TechBeat is always looking for good-quality photos that depict the many aspects of the law enforcement, corrections, and forensic sciences communities and illustrate the various tasks their personnel perform daily.

Photos should either be in color print or color slide format. Prints should preferably be 5 inches by 7 inches or 8 inches by 10 inches in size. Duplicate prints/slides made from originals—not the originals themselves—should be sent, as we cannot accept

responsibility for prints/slides that may be damaged or lost. Appropriate credit will be given to contributing photographers when their work appears in the TechBeat newsletter.

**Send your photographs, along with your name and daytime telephone number, to: Rick Neimiller, TechBeat Managing Editor, NLECTC, M/S 8J, 2277 Research Boulevard, Rockville, MD 20850. For more information, call 800-248-2742, extension 5432.**



TechBeat is the flagship publication of the National Law Enforcement and Corrections Technology Center system. Our goal is to keep you up to date on technologies that are currently being developed by the NLECTC system, as well as other research and development efforts within the Federal Government and private industry. Your questions, comments, and story ideas are always welcome. Contact: Rick Neimiller, managing editor, through NLECTC-National, 800-248-2742, or e-mail to asknlectc@nlectc.org. Additional copies of TechBeat are available at no cost. Writer and contributing editor, Lois Pilant. Reproduction of any part of this publication is encouraged by NLECTC unless otherwise indicated.



Photo © Stephen Agricol/Stock, Boston/PNI.

# Whatcha Gonna Do

**J**ust before 7 a.m. on an April day in 1992, officers from the U.S. Marshal's Service, along with three Montgomery County, Maryland, police officers, burst into a home in a Washington, D.C., suburb. As the officers came into the house, one of their "ride-alongs," a photographer from The Washington Post, began taking pictures of the residents: a man, Charles Wilson, dressed only in underpants, and his wife, Geraldine, dressed in a negligee. The officers were not there to arrest the couple. Instead they were after the couple's son, Dominic, believing that the house's address was also his. The Wilsons' son was wanted for violating probation on felony charges of robbery and assault. But Dominic was not at their house at the time of the raid. He did, however, turn himself in later at the urging of his parents.

Case closed?

Not quite. Although the photographs were never published, the couple sued the law enforcement officers involved in the raid. The Wilsons contended that the officers had violated their right to privacy under the Fourth Amendment by allowing a photographer as well as a reporter to enter the house.

In recent years, the practice of media "ride-alongs" with law enforcement, popularized on such television shows as "COPS," have become a public relations tool

to dramatize the activities of police departments across the country. However, the U.S. Supreme Court recently ruled that this practice could very well place officers at risk of having to pay monetary damages.

Citing a centuries-old principle of respect for the privacy of the home, in May 1999 the Court found in *Wilson v. Layne* that during the execution of a warrant, the presence of third parties unrelated to the actual execution of the warrant, such as a member of the media, is a violation of the Fourth Amendment rights of the homeowner and would allow the homeowner to seek monetary relief from the officers conducting the search or arrest. In siding with the Wilsons, the Supreme Court held that the Fourth Amendment requires that police actions in the execution of a warrant be related to the objectives of the authorized intrusion. The Justices determined that the presence of reporters was not related to the objective of the authorized intrusion because the reporters did not assist police in the execution of the warrant.

Law enforcement representatives presented several reasons to justify the media being allowed to accompany law enforcement officers during arrests. But the Court found that the reasons stated, which included minimizing police abuses, fell short of permitting a Fourth Amendment exception.

According to James H. Falk, Sr., chair of the National Institute of Justice's National Law Enforcement and Corrections Technology Center Liability Panel, the decision does not totally bar ride-along programs. Falk says that it appears to still be permissible to have members of the media accompany officers in situations that are of a public nature, where the expectation of privacy is not present, rather than in or around a person's private residence. However, he says, this "public versus private" line must be clearly drawn to prevent any liability concerns for officers.

Falk says that for departments that desire to videotape arrests for quality control or evidentiary purposes, the Court did stress the continued permissibility of that practice as long as the individuals videotaping the scene were law enforcement personnel and that the videotape generated remained the property and possession of that law enforcement agency. This, he says, is in accordance with the permissibility of the use of mounted video cameras on police cruisers to record the details of traffic stops.

**For more information or guidance on media ride-along programs, law enforcement agencies are advised to consult their own municipal counsel, as local laws may differ in regards to some aspects of these issues. James H. Falk, Sr., is an attorney with the Falk Law Firm in Washington, D.C., and is a trial and appellate advocate on constitutional law issues.**

National Law Enforcement and  
Corrections Technology Center  
P.O. Box 1160  
Rockville, MD 20849-1160

PRESORTED STANDARD  
U.S. POSTAGE PAID  
JESSUP, MD  
PERMIT NO. 4030

Please Route To:

Training Unit