Patrol officers are familiar with the routine: keying in a license plate number and waiting for the database to notify them of any alerts against the plate. A two-officer patrol team might run 100 or so license plates during a shift and, with luck, get a hit now and then. But now, using automatic license plate recognition technology, officers can run thousands of plates a day.

License plate recognition is an image-processing technology that reads a vehicle’s license plate, according to Tim McFadden, a project manager at the Office of Law Enforcement Technology Commercialization (OLETC), a program of the Office of Justice Programs’ National Institute of Justice (NIJ). OLETC offers commercialization assistance to companies that develop technologies and products for the public safety community.

"Once a license plate is read," McFadden says, "any number of applications are possible, such as allowing a vehicle access to an area, monitoring its entrances and exits, or checking it against databases tied to license plates. Currently, license plate readers are most often used in security and traffic applications for access control, but they are gaining in popularity due to availability of inexpensive cameras, smaller and more powerful computers, and the expanding need for security. The technology is increasingly being found in the areas of homeland security, tax enforcement, asset protection, special investigations, and fleet management."

According to McFadden, recent advances in data and technology have enabled vendors to develop new systems that can help law enforcement locate stolen vehicles, respond to AMBER Alerts and protect children from potential predators, and provide more effective border security.

The typical automatic license plate recognition system uses infrared light to illuminate a plate even in dark conditions. A high-speed camera photographs the plate, which is analyzed and compared with a database. The system alerts officers to any matches. Older scanning systems used a trigger mechanism, but newer systems can continuously run in the background. These systems received a boost in 2004 when the FBI’s National Crime Information Center created a process to provide agencies with a data extract, updated daily, of stolen vehicles, stolen plates, and wanted individuals for use with the systems.

The most obvious use for such systems is combating the $8 billion-a-year auto theft problem in the United States. The Pennsylvania Auto Theft Authority administers an insurance-funded program that supports auto theft units in Pennsylvania. Roy Miller, director of the authority, says that all participating departments are enthusiastic about the technology.

"In all instances, when they go out to test this technology, they are coming back with hits," Miller says. "This technology is going to knock auto thieves on their heels. Technologically, this stuff is ready."
Sgt. George Jacobs of the Maryland State Police heads the 34-officer Washington Area Vehicle Enforcement Unit (WAVE), a multijurisdictional task force that fights auto theft in the Washington, D.C., metropolitan area. Jacobs says the WAVE unit field tested systems from five vendors before buying one, noting that, “We recovered 8 cars, found 12 stolen plates, and made 3 arrests in just one shift during field testing.”

Automatic license plate recognition can also help police locate individuals who venture into prohibited areas, such as convicted sexual predators who come too close to a school or someone who comes too close to a residence in violation of a restraining order. Systems can call on integrated global positioning system (GPS) capabilities to issue an alert if an offender’s license plate is located in a restricted area. If license plate images and GPS locations are saved, that information can later be mined to create a list of potential witnesses and suspects.

Although the technology has many potential uses, it faces both technical and legal challenges. Technical challenges include differentiating between license plates from different States and dealing with obstructions. If two States have issued “ABC–123” as a license number, the system might issue an alert on a car from State A whereas the stolen vehicle is from State B. Vanity plates are especially susceptible to this problem, so officers must confirm alerts before acting on them. Trailer hitches, ice and snow, and plate covers can obstruct the camera’s view. Generally, if an obstruction prevents an officer from seeing the numbers and letters on a plate, a license plate reader will not be able to “see” it either.

McFadden notes other technical considerations in choosing a system. “Agencies considering purchases need to think about the types of vehicles they use, whether they want to maintain data for further analysis, and how frequently they plan to use their system,” he says. “For instance, certain systems require permanent mounting. If the department does not plan to dedicate a vehicle to license plate reader use, they should consider purchasing a portable unit. On the other hand, some agencies may plan to mount fixed units at toll booths or on highway overpasses, or use mobile units for covert operations.”

Legal challenges include privacy concerns as well as possible misidentification. “Every agency needs to make sure that it has a clear privacy policy and that it follows that policy in using this technology,” says Chris Miles, NJ senior program manager. “Used correctly, this technology has the potential to remove concerns over profiling of drivers because it analyzes every license plate seen, without concern for who the driver is.”

Miles also warns agencies to be careful when using technology that connects a person’s identity with a license plate number. The driver or passenger may not be the registered owner or the person for whom a warrant was issued, or out-of-date data may lead officers to stop a legitimate vehicle owner for operating a stolen vehicle. Officers therefore need to match not only the license plate, but also the driver’s identity before making a stop. Other policy considerations that Miles notes include probable cause for stops, data retention, evidence handling, and training.

In the end, Miles says, “Even though the systems still have some drawbacks, more and more law enforcement agencies are considering their purchase as an investigative tool.”

For more information regarding license plate reader technology initiatives being conducted by the National Institute of Justice and the Office of Law Enforcement Technology Commercialization, contact Tim McFadden, 888-306-5382 or tmcfadden@oletc.org.

The following table lists providers of automatic license plate recognition systems in the United States. This listing may not be inclusive nor does it constitute product endorsement by the National Institute of Justice or the U.S. Department of Justice.

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoVu Technologies</td>
<td>AutoPatrol™</td>
</tr>
<tr>
<td>Civica</td>
<td>Platescan™</td>
</tr>
<tr>
<td>DataWorks Plus</td>
<td>TAG-NABIT</td>
</tr>
<tr>
<td>Extreme CCTV</td>
<td>REG-RK-M1™</td>
</tr>
<tr>
<td>G2Tactics, Inc.</td>
<td>GLAVID™</td>
</tr>
<tr>
<td>Pips Technology</td>
<td>Pagis™</td>
</tr>
<tr>
<td>Remington Elsag</td>
<td>Mobile Plate Hunter</td>
</tr>
</tbody>
</table>

Because California’s Los Angeles Police Department (LAPD) has fewer officers per capita than other major cities such as Chicago or New York, Charlie Beck, assistant to the director, Office of Operations, is always on the lookout for technology solutions to help officers work more effectively. Knowing about the license plate recognition systems in place in Great Britain and Western Europe, Beck decided such a system could become a great tool for the department.

Beck, a former division captain, originally used grant money to purchase a system for his division. It worked so well that it helped earn him a promotion and the task of finding technology for the entire department.

“It offers huge advantages over the way we currently do it,” Beck says. “Even on a good day, a 2-person car can run 100 to 120 plates. With this system, we can scan upward of 1,000 plates an hour. The results have been pretty spectacular. An officer who tries to specialize in finding stolen plates might find one or two a month. With this technology, we sometimes get two or three a day.”

LAPD received technology demonstrations and evaluated equipment from four vendors and is now working on a request for proposals (RFP) to design its own system. Beck says LAPD would like a more user-friendly system for less technology-savvy officers. However, he says, the technology portion already works well. Cameras mounted in five field-test vehicles continuously scan lanes on the right, on the left, and in front of the car, comparing them with the 110,000 entries in a California Department of Justice database of stolen vehicles that is updated daily.

“This is something we’re really excited about, how many major crimes could be solved by applying this technology,” Beck says. “Parking checkers could use this instead of making chalk marks on tires. Fixed cameras could be installed in high-crime areas. It could be a huge tool in shopping malls, where we could drive through the parking lots and possibly find stolen vehicles. The law enforcement applications are just tremendous.”

Beck plans to have the RFP for LAPD’s system out to companies soon. He hopes license plate reading systems can one day be combined with in-car video, making police cars even more effective “offices.”

For more information on the Los Angeles Police Department's experience with license plate recognition technology, contact Charlie Beck at smartcar@lapd.lacity.org.
CATCH—the Crime Analysis Tactical Clearing House—supports law enforcement agencies in analyzing crime series and patterns. CATCH is a project of the Office of Justice Programs’ National Institute of Justice’s Crime Mapping and Analysis Program (CMAP) operated by the National Law Enforcement and Corrections Technology Center (NLECTC)—Rocky Mountain at the University of Denver.

According to Sean Bair, CMAP program manager, the CATCH project has a threefold mission: to provide technical assistance relating to serial crime, to warehouse serial crime data, and to make the data available for use in research and methodology development. Bair adds that data used for research and methodology development has been sanitized; that is, personal information relating to the perpetrator has been removed.

“The purpose of CATCH is not for us to become crime analysts for hire, but to ‘teach a man to fish’; that is, teach law enforcement departments to do their own crime analysis,” Bair says. He notes that CATCH staff use a number of crime mapping and analysis software applications and techniques to help agencies analyze identified crime series. He further notes that building up a warehouse of solved and unsolved crime series will provide researchers and theoreticians with reliable access to these data, enabling them to help agencies improve their methods of crime analysis and solve crime series more systematically.

Bair says that sanitized versions of closed crime series will generally be made available to requesters. Sensitive data and open cases may be made available to accredited researchers who assist agencies with ongoing crime series at the agency’s signed request.

The CATCH project evolved from a University of Denver graduate student thesis on next-event forecasting, which differs from geographic profiling. Geographic profiling analyzes the locations of a series of crimes to determine where the offender most likely resides. Next-event forecasting looks at where previous crimes occurred to predict where the next crime will happen.

CATCH is now available to law enforcement nationwide following its beta test debut in the Four Corners States [Utah, Colorado, New Mexico, and Arizona] during 2005.

“Before opening up the project to the entire country, NLECTC—Rocky Mountain wanted to run CATCH on a trial basis,” Bair says. “We wanted to see how it worked out in a smaller area first. We knew if we just made a broad announcement, we would be inundated. Late in 2005, we expanded the project into a few other States.

“The beta phase was a time to streamline the process. We wanted to gauge how much time it would take to work with a department and show their people what could be done, what couldn’t be done, and how their own staff could do it themselves next time. It turns out that the average time spent on cases varies between 2 and 4 hours.

“In addition to showing law enforcement agencies how to use the techniques of the CATCH project for future serial crime cases, we are encouraging agencies to take advanced CMAP training, all aimed at making their use of CATCH a one-time event. Also an important part of CATCH is determining if a particular department’s crime series is an extension of what is going on in someone else’s jurisdiction.”

For example, Bair says, more than 200 burglaries have occurred in the Colorado Front Range, all believed to have been committed by the same suspect and spanning the jurisdictions of approximately 10 police departments.

“Our approach has been to help them by facilitating communication across the various agencies. With so many cooks in the kitchen, there isn’t necessarily one cook who holds the recipe. Initially, we invited all the agencies together, provided them the venue to meet and discuss the series, and helped facilitate the cross-jurisdictional analysis.

“We also have helped them deal with the technological issues that came about because of the size of this series, which crossed so many boundaries. It is difficult to put the whole series on one map. We have helped them see the puzzle by putting together its individual pieces, and we assisted them with the analysis of the series and provided feedback on what to look for. That is a very typical example of what we’re able to do from a technological standpoint.”

For more information on the CATCH project, contact Sean Bair at 800–416–8086 or sbair@du.edu. Or visit www.crimeanalysts.net/catch.htm. For general information about the CMAP initiative, visit www.crimeanalysts.net.
Once they left their homes and lurked around playgrounds and malls. Now, they stay at home and frequent online chat rooms. Some pretend to be younger, or even a different sex. Either way, their intended prey is the same: the young and innocent. Moreover, their use of the Internet makes them hard to catch.

Recent news stories have reported the dangers of unsupervised use of the Internet by children and adolescents: young girls lured into meeting online friends who turn out to be older men; boys thinking they are chatting with teenage girls, all the while revealing their secrets to sexual predators. But other dangers lurk on the Internet: bullying, hate mail, and persecution—often by other teenagers—are being taken to new levels.

According to i-SAFE America, 42 percent of children surveyed in 2004 said they had been bullied online, 35 percent said they had been threatened online, and 21 percent said they had received mean or threatening messages online. A study by the National Center for Missing & Exploited Children revealed that one in four children between the ages of 10 and 17 has been exposed to unwanted sexual material online.

Parents often know less about how their computers work than their children do, and they have no idea of the dangers their children face. Generally, law enforcement officers are aware of these dangers from bulletins and alerts, but they often have no idea how to combat them. That, according to Senior Engineer Jeffrey Isherwood, is where the Office of Justice Programs’ National Institute of Justice’s (NIJ’s) CyberScience Laboratory (CSL), located at the National Law Enforcement and Corrections Technology Center—Northeast in Rome, New York, can assist.

Isherwood explains that CSL, part of NIJ’s Electronic Crime Program, works with law enforcement officers to present seminars on Internet and child safety for parents and the community. Law enforcement agencies promote the seminars and provide the audiences, and CSL helps provide content, either in person or through detailed technical assistance, that makes a variety of electronic media and information resources available to law enforcement agencies.

CSL has produced a series of posters and desktop reference cards for practitioners, parents, and educators. Isherwood says. Titles include “A Parent’s Guide to Child Internet Safety,” “Multimedia Storage Devices,” and “Wireless Security Tips.” Other cards cover steganography (hiding data inside other data) and identity theft. Another resource is the U.S. Secret Service’s Forward Edge II, a multimedia CD-ROM with several electronic crime-training scenarios, including one where an Internet predator stalks a 13-year-old girl, hiding his identity via a neighbor’s residential wireless network.

“These activities and resources are part of our overall fight against cybercrime,” Isherwood says. “It comes down to understanding the technology. Online crimes against children are cybercrimes, and we help law enforcement with cyber investigations of all types. Children are our most precious asset. Which cybercrime can hurt a family more: identity theft or child exploitation?”

CSL also offers seminars on gathering electronic evidence, one of which, Isherwood says, led to a recent arrest in Missouri City, Texas. An investigator who had attended a CSL-sponsored seminar remembered information presented on the miniaturization of storage devices and used her newfound knowledge to locate a piece of electronic evidence that held child pornography. In another case, a New York State trooper who had attended a steganography seminar collaborated with the U.S. Border Patrol to advance an investigation of a Level III (habitual repeat) sex offender trying to cross the border with several suspicious computer-related items.

“When you talk about a crime against a child on the Internet, it’s the same kind of investigation and

An INTER(safety)NET

NIJ Electronic Crime Program

Based on needs identified by the law enforcement and public safety community in the Office of Justice Programs’ National Institute of Justice’s (NIJ’s) Electronic Crime Needs Assessment for State and Local Law Enforcement, NU’s Electronic Crime Program addresses any type of crime involving digital technology, including cybercrime and cyberterrorism. The goal of the program is to enable the criminal justice community to better deal with electronic crime through development of improved tools and technologies and by building capacity for and conduits among Federal, State, and local agencies; industry; and academia. For more information, including a list of downloadable electronic crime publications, visit www.ojp.usdoj.gov/nij/sciencetech/welcome.html.

i-SAFE America

i-SAFE America, Inc., is the worldwide leader in Internet safety education. Founded in 1998 and endorsed by the U.S. Congress, i-SAFE is a nonprofit organization dedicated to protecting the online experiences of youth everywhere. i-SAFE incorporates classroom curriculum with dynamic community outreach to empower students, teachers, parents, law enforcement, and concerned adults to make the Internet safer. For more information, including information and resources for law enforcement, visit www.isafe.org.

The National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children’s mission is to help prevent child abduction and sexual exploitation, help find missing children, and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them. The Center was established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in preventing the abduction, endangerment, and sexual exploitation of children. For more information, visit www.missingkids.com or call 703-274-3900.
It was the worst snowstorm to strike Regina, Saskatchewan, in 25 years—a blizzard that stranded travelers and shut down the Trans-Canada Highway. But it was perfect weather for testing winter tires.

Law enforcement officers in northern climates must drive in snow, ice, extreme cold, and other hazardous conditions. Therefore, proper winter tires are important for vehicle handling, according to Bruce Richter, deputy director of the National Law Enforcement and Corrections Technology Center (NLECTC)—Northwest in Anchorage, Alaska, which is a program of the Office of Justice Programs’ National Institute of Justice.

To help law enforcement agencies select the right winter tires, NLECTC—Northwest and the Canadian Police Research Centre tested five brands on snow-covered test-driving tracks at the Royal Canadian Mounted Police (RCMP) Depot in Regina in February 2004. The RCMP Depot’s driver training unit provided the test vehicles and trained law enforcement driving instructors to operate them. Depot staff also provided logistical, mechanical, and test track preparation support. Ford Motor Company, the U.S. Army Cold Regions Research and Engineering Laboratory, and the Tekne Group, Inc., also took part.

Brands tested were the Continental ContiWinterContact TS790, Firestone Firehawk PVS, Goodyear Eagle Ultra Grip GW2, Michelin Pilot Alpin, and Pirelli Winter 210 Snowsport. The manufacturers submitted samples of commercially available, nonstudded winter tires sized for the rear-wheel-drive Ford Crown Victoria Police Interceptor. All winter tires tested were certified as meeting the North American Rubber Manufacturers’ (www.rma.org) severe snow standard and were rated for law enforcement driving speeds.

RCMP used two 2003 Police Interceptors in testing; each test run took place on fresh snow. Data acquisition systems in the vehicles recorded time, distance, and acceleration. All winter tires were measured against a set of control tires—the Goodyear Eagle RS–A Plus, an all-season pursuit speed rated tire that is original equipment on the Police Interceptor. Periodically running the control tires through the test helped testers determine a baseline and evaluate whether temperature, wind, fresh snow, humidity, and sunshine conditions had changed.

All five brands of winter tires consistently outperformed the control set of all-season tires. “As good as they are, all-season tires are a design compromise,” Richter says. “Winter tires have specially designed tread patterns and are made of rubber compounds that deliver superior performance in cold weather or snow.” These special tread designs include a large number of tread sipes (small cuts or grooves in the tread block) for wet surface control and an open tread block pattern for better deep snow traction.

The testing also showed that any set of four matched winter tires provided better performance than placing winter tires on the rear wheels only. Richter says mismatched tires caused unstable vehicle handling. (Using only two winter tires to reduce tire costs proves to be a false economy.)

All the brands of tires tested are designed for temperatures between −15 and −4 degrees Celsius (5 to 25 degrees Fahrenheit). Temperatures during testing were often lower, at times reaching −40 degrees Celsius (−40 degrees Fahrenheit). Tests conducted at warmer temperatures could produce different results.

For more information about the methodologies and results of this winter tire testing initiative, visit www.nlectc.org/testing/wintertires.html, or contact NLECTC—Northwest, 866-569-2969 or nlectc nw@ctsc.net. For information about other patrol vehicle tire testing initiatives conducted by the NLECTC system, visit www.justnet.org/testing/tires.html.
The National Law Enforcement and Corrections Technology Center (NLECTC) system, a program of the Office of Justice Programs’ National Institute of Justice (NJI), offers no-cost assistance in helping agencies large and small implement current and emerging technologies.

The NLECTC system was established in 1994 by NJI’s Office of Science and Technology to serve as an “honest broker” resource for technology information, assistance, and expertise by providing information and technology assistance to the Nation’s more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probation departments; and other public safety organizations.

With a network of regional centers and specialty offices located across the country, the NLECTC system delivers expertise in a number of technologies in partnership with a host organization. In addition, a number of technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for each of NJI’s technology focus areas.

Contact NLECTC for:

Technology Demonstration
We introduce and demonstrate new and emerging technologies through special events, conferences, and practical demonstrations as the Mock Prison Riot (technologies for corrections) and an annual public safety technology conference. On a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Capacity Building
We provide hands-on demonstrations of the latest technologies to address such operational issues as crime and intelligence analysis, geographic information systems, explosives detection and disablement, and semi-automatic pistols is tested on a pass/fail basis. NLECTC also conducts comparative evaluations—testing equipment under field conditions—on patrol vehicles, patrol vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves. NLECTC also has evaluated pads; and cut-, puncture-, and pathogen-resistant gloves. NLECTC also has evaluated pads; and cut-, puncture-, and pathogen-resistant gloves.

Property Acquisition
We help departments take advantage of surplus property programs that make Federal equipment is safe, dependable, and effective.

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, news summaries, meeting/conference reports, videotapes, and CD-ROMs. NLECTC also publishes TechBeat, an award-winning quarterly newsmagazine. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, 800–248–2742, or via e-mail at asknlectc@nlectc.org.

Technology Commercialization
Our law enforcement and corrections professional, product and commercialization managers, engineers, and technical and market research specialists work together to identify new technologies and product concepts. They then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.

Technology Needs Assessment
Our national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—ensures that we are focusing on the real-world needs of public safety agencies.

Because most of the country’s law enforcement and corrections services are provided at the local level, the NLECTC system is composed of five regional centers and is complemented by several specialty offices and a national center. Most centers and offices are colocated with or supported by a number of technologies in partnership with a host organization. In addition, a number of technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for each of NJI’s technology focus areas.
Simulating More Than a Game

A new simulation software program called Incident Commander allows first responders, especially those in small and rural departments, to get the feel of hands-on simulation training. Currently in beta version, this free CD-ROM includes scenarios such as a chemical spill resulting from a train derailment, a bomb threat in a courthouse, and a school hostage situation. Developed for NIJ by a games development company with guidance from a team of subject matter experts from across the country, the software can be used by 3 to 16 players. Scenarios start partway into an incident, and how the scenario unfolds depends on participants’ decisions. For example, during the school hostage scenario, if the incident commander does not establish a perimeter, representatives of the media enter the school, with the potential to broadcast damaging information about the incident or become hostages themselves. Incident Commander will be released at no cost by NIJ following final review and approval. More information about Incident Commander call 720–470–7576 or e-mail cathleen.strabala@ dolphotech.com.

Hiding Evidence Offsite

If the task of searching for evidence on a computer wasn’t hard enough with the various ways of hiding data, a new twist on an old idea has made it even more difficult. Offsite data storage is a costly security measure that has been used by companies for many years. Recently, software programs have been developed that manipulate free Web services, such as e-mail accounts or databases, and allow anyone with a computer and Internet access to store files offsite at no cost. This remotely stored data could include child pornography, sale of narcotics spreadsheets, stolen credit card information, or other potential evidence at an offsite location without the service provider’s knowledge. Some software programs even encrypt the data, then store the potential evidence offsite on another machine.

To obtain a threat assessment report that describes offsite evidence in greater detail, go to www.cybersciencelab.com (registration on the Private Site is required to complete the download), or contact Derek Larson, an economic crime specialist at NIJ’s CyberScience Laboratory in Rome, New York, at Derek@ dolphotech.com.

Picture of the Golden Gate

NLECTC–West is currently supporting the Golden Gate Safety Network (GGSN) in the development of a common operating picture that can locate and track multiagency assets. This past November, NLECTC–West produced a prototype system for demonstration during a GGSN tabletop exercise. The system collected GPS location information from a variety of devices using different communication links. The location of the GPS devices was plotted on a Google® map available via the Internet to all participants. At the conclusion of this multiyear project, NLECTC–West will produce shareware to generate a common operating picture of vehicles and vessels operating in a mutual aid situation.

GGSN was formed several years ago as an informal means for San Francisco Bay Area private and public safety groups to collaborate on regional incident management coordination and response planning. Following several tabletop and field exercises, the group recognized the need for an ongoing effort to promote incident management data sharing through the use of emerging technologies and current off-the-shelf and nonproprietary equipment and systems. As part of this effort, NLECTC–West, the California Governor’s Office of Emergency Services, and the Marin County (California) Sheriff’s Office have entered into a memorandum of agreement to support GGSN efforts. For more information, contact NLECTC–West, 888–548–1618 or nлектc@faw-west.org.

Getting SMART

The objective of SMART Briefs, a project of NIJ’s Rural Law Enforcement Technology Center located in Hazard, Kentucky, and Eastern Kentucky University’s Justice and Safety Center, is to collect and disseminate information about new technology of interest to small and rural police agencies nationwide. The first SMART Brief was a survey conducted last summer that looked at the adoption of digital technology (cameras and audio and video recorders) by these departments, how the departments obtained digital evidence, and how they used the evidence in court. Overall, the findings showed most agencies have little difficulty with the admissibility of digital evidence; however, methods for storing digital evidence vary widely, indicating a need for the development of standards, technology, policies, and procedures. The biggest impediment to further adoption of digital technology by small and rural agencies is cost.

According to the brief, two issues bear watching when it comes to the use of digital cameras and recorders by small and rural law enforcement agencies. First, digital photographs and recordings have not been challenged very often in court. They also have not been presented to higher court judges very often. Therefore, it is possible that legal challenges will become more common as attorneys become familiar with threats to the reliability and validity of digital images and as it becomes more certain in serious cases in the higher courts to incorporate such evidence. Second, it seems that standard methods for storing digital photographs and recordings have not been adopted yet by the law enforcement community. As legal challenges increase, it will become even more important to be able to prove the chain of custody of digital evidence. Also, over time, even small and rural agencies will accumulate more and more digital evidence, making it necessary to implement systematic and legally sufficient storage systems. Otherwise, digital evidence will get lost or corrupted, leading to embarrassment and failed cases.

For a copy of the SMART Brief on digital technology use by small and rural law enforcement departments, contact Gary Cordner at gary.cordner@eku.edu, or call 859–622–8484.

Handcuffs With Memory

NIJ’s Office of Law Enforcement Technology Commercialization is providing assistance to the developer of a disposable handcuff system that integrates a USB-compatible, 128-megabyte digital data storage device with a disposable handcuff system. With this handcuff system, any type of digital data, including e-forms, photographs, audio, video, and biometrics, can be securely transported with the arrested person, assuring a complete chain of identity for the suspect and trackable custody for records and evidence. For more information, contact Tim McFadden at 888–306–5382 or tmcfadden@nlectic.org.
The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #2005–MU–CX–K077 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 Lockheed Martin Aspen Systems. 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.

The U.S. Department of Justice, Office of Justice Programs’ National Institute of Justice, in association with CIC, Inc.–Public Safety Technology Center, presents the 8th Annual Technologies for Critical Incident Preparedness Conference and Exposition September 6–8, 2006, at the Hyatt Regency in Atlanta, Georgia.

Following on the success of last year’s conference in San Diego, this conference will highlight current and under-development technology and training specifically for the first responder. Tentative breakout session topics will include the following:

- Incident Command
- Communications Interoperability
- NIMS Compliance
- Information Sharing
- Border and Transportation Security
- Critical Infrastructure Protection
- Federal Resources
- Risk Assessment
- Electronic Crime and Cyber Security
- CBRNE Countermeasures
- Emergency Medical Services
- Personal Protective Equipment
- Search and Rescue
- Forensics

With more than 1,000 attendees and 150 exhibits expected, the conference and exhibition will offer a unique opportunity for first responders, business and industry, academia, and elected officials to network, exchange ideas, and address common critical incident technology and preparedness needs and solutions.

For hotel reservations and attendee registration, visit www.ctc.org. There is a 10 percent early registration discount for attendee registrations that are paid in full before July 1, 2006.

To obtain more information or view last year’s conference program, visit www.ctc.org. Additional information will be posted on the conference website as the agenda and speakers are confirmed.

NCJRS Contact Information at a Glance
Web: http://www.ncjrs.gov
Phone: 800–851–3420 (Monday – Friday, 10 a.m. to 6 p.m. e.s.t.)
Fax: 301–519–5212
Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–6000

The National Criminal Justice Reference Service

In addition to funding the National Law Enforcement and Corrections Technology Center, the National Institute of Justice (NIJ) and other Federal agencies support the National Criminal Justice Reference Service (NCJRS), assisting a global community of policymakers, practitioners, researchers, and the general public with justice-related research, policies, and programs.

NCJRS offers reference and referral services, publications, onsite and offsite conference support, and other technical assistance. The easiest way to access NCJRS is online.

The NCJRS website showcases the latest criminal and juvenile justice and drug policy information. Take advantage of—

- Topic-specific resources.
- Online registration and ordering.
- Searchable abstracts and calendar of events, and questions and answers databases.

Stay informed. Register at http://www.ncjrs.gov/subreg.html to receive—

- JUSTINFO. A biweekly electronic newsletter that includes links to full-text versions of printed publications.
- E-mail notifications. Periodic messages about new publications and resources that match your specific interests.

Additional information will be posted on the conference website as the agenda and speakers are confirmed.
I

n 2005, the most active hurricane season on record, Hurricanes Katrina and Rita pounded a large portion of the Gulf Coast. Winds and rain caused widespread flooding, washing out roads and bridges and contributing to the loss of utility services and communications. In their wake, the storms left immeasurable commercial and residential property damage and tens of thousands of people homeless.

First with Hurricane Katrina, and then a month later Hurricane Rita, law enforcement agencies in the devastated areas of the Gulf Coast had all that they could handle coping with looters, helping to rescue stranded persons, and ensuring the public safety.

Their mission, however, was made a little easier through the efforts of the National Law Enforcement and Corrections Technology Center (NLECTC)–Southeast, which provided computers and other supplies from the U.S. Department of Defense’s 1033 Program to the storm areas. NLECTC–Southeast is a program of the Office of Justice Programs’ National Institute of Justice.

NLECTC–Southeast’s Ken Dover, program manager for the Center’s Excess Federal Property Program, knew law enforcement agencies in the hard-hit States of Louisiana and Mississippi would need computer equipment in the wake of the storms. Using the 1033 Program, which permits the Secretary of Defense to transfer excess U.S. Department of Defense supplies and equipment to State and local law enforcement agencies without charge, Dover located computers in Missouri and Illinois. He picked up the computers, keyboards, monitors, and mice in Springfield, Illinois, helped load them on a truck, then drove them to Baton Rouge. Before distribution there, he reinstalled operating systems and ensured that the computers were in working order. In all, Dover secured 160 computers for use in Louisiana and 180 in Mississippi.

“For most of the law enforcement agencies in both States, their complete computer systems were gone,” Dover says. “Our assistance was basically a cooperative effort between several States and the 1033 Program to get the agencies up and running again. We put out the word to all 1033 Program State Coordinators to be on the lookout for computers. They in turn contacted Department of Defense units in their State.”

In addition to the computers from Missouri and Illinois, the Gulf Coast States received other supplies from out of State. “For example, North Carolina Law Enforcement Support Services maintains a contingency stock for disaster relief. The week after Katrina, they sent three tractor-trailer loads of cots, food, and clothing,” Dover says, adding that Georgia also sent cots.

Additional NLECTC–Southeast assistance to law enforcement came from Charles Stephenson, a project manager at the Center. Stephenson was deployed to Houston following Hurricane Rita to help with communications interoperability issues. There, he trained Texas Department of Public Safety staff on the use of interoperability gateway switches that NIJ provided. He worked to restore communications in the Beaumont area and establish communications interoperability among the Texas Department of Public Safety, the U.S. Air Force, and the Beaumont Police Department. From Houston, Stephenson moved on to collaborate with NIJ staff in bringing in supplies and helping to solve communication issues in Jasper County, Texas.

“We actually were set up at the airfield in the county, where we helped receive and issue the supplies,” says Stephenson, adding that NIJ offered communications assistance following Katrina, but conditions proved so chaotic in New Orleans that local law enforcement was not sure how to use the help. “Katrina kind of hit the area by surprise. There wasn’t a mechanism in place to use what was being offered. Following Rita, things went more smoothly.”

For more information about the 1033 Program, contact Ken Dover, 888–874–5854 or kdover@nlectc-se.org. For more information about NLECTC–Southeast communications technology initiatives, contact Charles Stephenson, 843–760–3283 or stephenson@nlectc-se.org.
TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

**Individual Subscriptions:** TechBeat is available at no cost. If you are not currently on our mailing list, please call us at 800–248–2742, fax 301–519–5149, or e-mail us at asknlectc@nlectc.org.

**Domestic Department Subscriptions:** If your division, department, or agency has more than 20 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no Post Office boxes, please), and a contact name and telephone number. Your only obligation is to disseminate them once they arrive. If you require fewer than 20 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742 for additional information or to subscribe.

**Address Correction:** Please notify us of any change in address or point of contact. Call 800–248–2742; fax 301–519–5149; or e-mail asknlectc@nlectc.org.

**Article Reproduction:** Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as, “This article was reproduced from the Spring 2006 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

**Awards:** TechBeat has received numerous awards, including the 1998 Best of Category, Excellence in Printing Award from the Printing & Graphic Communications Association; the first-place 1998 Blue Pencil Award for Most Improved Periodical from the National Association of Government Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; and the APEX 2001 Award of Excellence for Magazines and Newspapers–Printed.

**Photo Credits:** Photos used in this issue of TechBeat copyright © 2006 Alamy; Clipart.com; Corbis Images; Getty Images; Veer; Photodisc; ImageState; and Fotosearch.

**Address Correction:** Please notify us of any change in address or point of contact. Call 800–248–2742; fax 301–519–5149; or e-mail asknlectc@nlectc.org.

**Website:** www.justnet.org

**Online News Summary.** Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major newspapers, magazines, and periodicals and on national and international wire services and websites.

**Testing Results.** Up-to-date listing of public safety equipment evaluated through NIJ’s testing program. Includes ballistic- and stab-resistant armor, patrol vehicles and tires, protection gloves, handcuffs, and more.

**Publications.** Publications from NIJ and NLECTC that you can view or download to your system, including printer-friendly versions of TechBeat articles and features.

**Calendar of Events.** Calendar of Events lists upcoming meetings, seminars, and training.

**Links.** Links takes you to other important law enforcement and corrections websites.

For help establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800–248–2742.
Judges, lawyers, scientists and law enforcement are overwhelmed by the amount of science and technology information required to educate themselves to meet the many legal challenges. Navigating the vast terrain of information contained within the existing case law, scientific journals, reports, publications and other resources has been, in the past, an impossible task. The National Clearinghouse for Science, Technology and the Law assembles the available scientific, technological, and relevant legal resources into a comprehensive ‘one-stop’ searchable database with equal access for all.”

—From the website of the National Clearinghouse for Science, Technology and the Law.

A buzzword often heard in recent years is ‘one-stop shopping,’ or providing a comprehensive selection of goods or services at one location. Carol Henderson, director of the National Clearinghouse for Science, Technology and the Law, and her staff take ‘one-stop shopping’ seriously in carrying out their mission to help law enforcement personnel and others deal with the vast amount of science and technology information.

“There’s nothing else like it in the world.” Henderson says of clearinghouse resources, which include a vast Internet-accessible database, a library collection, an ongoing educational lecture series, and more. “I want to get the word out so people know about it and use it. It’s a one-stop shopping place for science, technology, and law resources.”

Henderson says the clearinghouse’s comprehensive online bibliographic database contains materials dating back to 2000 and includes court decisions and commentary, scholarly publications, commercial applications, books, journals, articles, information on professional associations and institutions, best practices and standards, and other resources pertaining to law, technology, and science. Funded by the Office of Justice Programs’ National Institute of Justice (NIJ), the clearinghouse has a mission of helping law enforcement personnel and others navigate that vast amount of information.

“Think of it as a giant online bibliography,” Henderson says. “You can research topics ranging from ‘traditional’ technology to cutting-edge science like biometrics.”

At last count, she says, the database contained more than 25,000 data entries. A full-time research director and research staff, including student interns, continuously update the database.

“We’re happy to take any contributions people want to make. If someone says I have a collection of forensic materials, I’d like to donate it to the clearinghouse, we’ll then make it available to many who otherwise would not have access to the information,” Henderson says. “It’s free; there’s public access; anyone can go and look at it.” In addition, staff have created specialized bibliographies on frequently researched topics, such as the “CSI effect” on jurors.

In addition to assembling the online database and corresponding hard copy library, which is located at the Stetson University Law School in Gulfport, Florida, the clearinghouse has other objectives as well, including producing an ongoing lecture series on science, technology, and the law. These one-session lectures can be attended in person, viewed live via a Webcast, or viewed later on DVD. Lectures address topics such as forensic pathology, the use of forensic science in human rights violations, new developments in forensic science, and more. Upcoming lecture dates and topics can be found on the clearinghouse website.

Other clearinghouse projects include:
- Hosting national conferences for NIJ on science, technology, and the law. (The next conference will be held November 2-5, 2006, in St. Petersburg, Florida.)
- Developing training modules, with an emphasis on distance education. (Law 101 is in development and provides an overview of the law, ethics, and other issues dealing with trial testimony.)
- Creating primers on law, science, and technology topics.

At last count, she says, the database contained more than 25,000 data entries. A full-time research director and research staff, including student interns, continuously update the database.

“We’re happy to take any contributions people want to make. If someone says I have a collection of forensic materials, I’d like to donate it to the clearinghouse, we’ll then make it available to many who otherwise would not have access to the information,” Henderson says. “It’s free; there’s public access; anyone can go and look at it.” In addition, staff have created specialized bibliographies on frequently researched topics, such as the “CSI effect” on jurors.

In addition to assembling the online database and corresponding hard copy library, which is located at the Stetson University Law School in Gulfport, Florida, the clearinghouse has other objectives as well, including producing an ongoing lecture series on science, technology, and the law. These one-session lectures can be attended in person, viewed live via a Webcast, or viewed later on DVD. Lectures address topics such as forensic pathology, the use of forensic science in human rights violations, new developments in forensic science, and more. Upcoming lecture dates and topics can be found on the clearinghouse website.

Other clearinghouse projects include:
- Hosting national conferences for NIJ on science, technology, and the law. (The next conference will be held November 2-5, 2006, in St. Petersburg, Florida.)
- Developing training modules, with an emphasis on distance education. (Law 101 is in development and provides an overview of the law, ethics, and other issues dealing with trial testimony.)
- Creating primers on law, science, and technology topics.

The clearinghouse also plans to convene community acceptance panels, or focus groups, of diverse participants to assist NIJ with its technology research agenda.

For more information about the resources and services offered by the National Clearinghouse for Science, Technology and the Law, visit www.ncstl.org, phone 727-562-7316, or e-mail Watson@law.stetson.edu.

The CSI Effect

Around the nation’s courthouses these days the term “CSI effect” can be heard. Spawned by such television series as CSI and its spin-offs CSI Miami and CSI New York, the CSI effect refers to the belief by the public that science is fast and infallible—just like it is portrayed in the many police and crime scene investigation programs airing in prime time.

According to numerous reports by the national media, the CSI effect is now influencing how lawyers are preparing their cases as well as the expectations that law enforcement and the general public are placing on crime laboratories. Real-world crime scene investigators say that CSI-type programs are giving the public unrealistic expectations of just what forensic sciences can currently deliver.
Isherwood notes that one type of computer-based crime that has made few headlines is cyberbullying. Cyberbullies, he says, follow their victims electronically, harassing them, insulting them, and/or posting demeaning photographs and text messages.

In addition to exploitation and bullying, Isherwood adds that law enforcement needs to be aware of all the dangers the Internet poses to youngsters. Adolescents may turn to hacking, or may buy cigarettes, liquor, drugs, and other harmful or illegal substances online. Most are not hard-core delinquents. They attempt such feats out of a sense of daring much as underage youth from earlier generations tried to purchase the same types of items in stores.

“Law enforcement officers, for the most part, know what the dangers are. The problem is conveying the message to parents,” Isherwood says. “You tell them that downloading music files is piracy and against the law, and they don’t understand that it really is wrong. It should be the responsibility of the parents to educate and protect their children in the online world. If they fail, law enforcement needs to be prepared to handle the results.”

For more information on child safety and Internet safety technical assistance and resources available from the CyberScience Laboratory, contact Jeffrey Isherwood, 312-838-7064 or ish@dolphtech.com, or visit www.cybersciencelab.com. Access to the full site requires registration.