Winter 2010

TECH beat

NLECTC
National Law Enforcement and Corrections Technology Center

A Program of the National Institute of Justice NIJ

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

Deployable Labs

It's a long way from Iraq to Cedar Rapids, from Afghanistan to the Upper Peninsula of Michigan. However, those four areas had something in common: a need to fight criminal activity by performing analysis, and no permanent structure to host a lab. A way of housing equipment to defeat improvised explosive devices overseas is now helping U.S. law enforcement agencies that need a temporary place to house their forensic resources.

Several years ago, Kevin Lothridge, presently director of the Forensic Technologies Center of Excellence (CoE), which is funded by the Office of Justice Programs' National Institute of Justice (NIJ), had the opportunity to observe the U.S. Navy's Combined Explosives Exploitation Cell (CEXC). Their use of mobile laboratories for improvised explosives device (IED) analysis activities struck him as a concept with potential to help the law enforcement community.

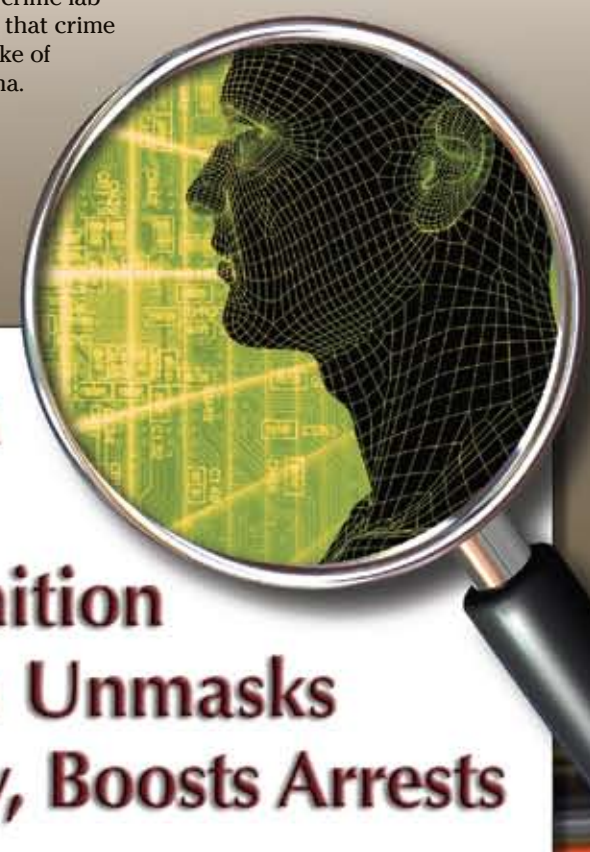
Lothridge, who also directs the National Forensic Science Technology Center (NFSTC) in Largo, Fla., (which hosts the CoE), saw possibilities for using these deployable forensics labs in time of need.

NFSTC helped refine the concept and began to move it forward, first creating a prototype and then a group of second-generation labs used extensively for training programs. Using NIJ funding and feedback based on their initial use, creation of third-generation units is underway. NFSTC's efforts were facilitated by an agreement between NIJ and the U.S. Department of Defense's Defense Threat Reduction Agency (DTRA) (see sidebar).

Lothridge describes the deployable labs as shipping containers that fold out. The self-contained labs have generators, heat, air conditioning and electrical hookups. Forensic equipment, if needed, can also be shipped inside the labs, which travel easily on a standard trailer. NFSTC loans them to qualified law enforcement agencies free of charge; the receiving agency need only pay the cost of transportation. Agencies may provide their own equipment but NFSTC will work with them on supplying loaner equipment to fill any anticipated gaps. Lab setup can be accomplished by three people in about an hour. If an agency needs additional space, two of the laboratories can be joined by a causeway.

"When I saw the CEXC demonstration, it was the year of the four major hurricanes (2005)," Lothridge says. "The city of New Orleans and other nearby areas had no crime lab capability, and we all know that crime tends to increase in the wake of natural disasters like Katrina. If the program had existed then, the labs could have been used to replace the capacity of a destroyed lab or enhance the capacity of the nearby labs that were overburdened. It's a great partnership going across DoD, NIJ and DHS [U.S. Department of Homeland Security], really a true technology transition opportunity."

(See Deployable Labs, page 3)



Florida Facial Recognition System Unmasks Identity, Boosts Arrests

Pulled over for running a red light, the driver tells the officer who stopped him that his name is John Smith and he must have left his wallet at home. Does the officer a) let him go with a warning, b) take him into the station for fingerprinting and further attempts at establishing his identity, or c) take his picture?

If the officer is a Pinellas County, Fla., sheriff's deputy, then "c" is the correct answer. After plugging the easy-to-use digital camera into the car's laptop, the deputy can continue to keep an eye on the driver while the computer automatically downloads the image, opens the sheriff's office facial recognition program, converts the image with a binary algorithm, runs a search of the county's database and produces a gallery of potential matches, all in less than 30 seconds.

It might turn out that the driver's name isn't John Smith after all.

Using initial funding provided through the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS), Pinellas County has adapted a facial recognition system that has grown from a replacement for the county jail's mug shot database into a partnership system that encompasses 14 of the state's 67 counties and could well serve as a model for similar systems in other states. The software was developed by Viisage of Massachusetts.

(See Florida Facial Recognition System, page 2)

Facial Recognition System ARRESTS

The Pinellas County Sheriff's Office facial recognition system has been responsible for hundreds of arrests annually, arrests that might not have been made without assistance from the system. Here are just a few examples:

- On July 1, 2009, the Sheriff's Technical Operations Unit received a request from the Miami Police Department for help with identifying a bank robbery suspect. The suspect provided Miami police with a homeless shelter ID. Pinellas County ran the image and within minutes came up with a booking photo match for the suspect, who had been previously arrested in Orange County, Fla., in 2003, under a different name. That image led to a positive identification of the suspect, who was arrested in St. Louis the next day.

- A deputy on patrol on Feb. 11, 2009, spotted a white Ford Explorer with an expired temporary tag. The deputy learned the registered owner's driver's license expired in 2007, and therefore pulled over the driver and two passengers for a routine traffic stop. The driver had no photo identification and claimed the vehicle belonged to a friend. The deputy used his facial recognition system and found no matches for the driver. The deputy then asked if either of the two passengers in the vehicle had a valid driver's license, and one provided a Guatemalan driver's license. The deputy then used facial recognition to attempt to identify the passenger and found three photos from previous arrests in Pinellas County under a different name. He located a record of an expired Florida driver's license for this subject and an active Pinellas County warrant for failure to appear for soliciting prostitution. The deputy took the suspect into custody.

- On May 7, 2009, a North Miami Police Department detective contacted the Pinellas County Sheriff's Office with a request for facial recognition identification of an attempted bank robbery suspect. Surveillance photos showed a man passing a note to a teller demanding money. When the frightened teller moved away from the window, the man left the bank. A search returned three potential matches — one from the Florida Department of Corrections and two from the Miami-Dade area. The man initially identified as the suspect was eventually arrested and confessed to the robbery attempt.

- On Sept. 11, 2004, Pinellas County deputies responded to reports of a disorderly female in a mobile home park. The woman could not provide identification and gave what deputies believed to be a false name. The responding deputies requested assistance from a facial recognition-equipped unit and that deputy took two digital pictures and submitted them to the facial recognition system. After receiving a gallery of photos, the deputy compared the photos to four possible matches. He determined that all four photos were the same person and located two outstanding Pinellas County warrants for the subject related to drug possession and prostitution.

(Florida Facial Recognition System . . . cont. from page 1)

Pinellas County Capt. Jim Main explains that when the project started in 2001, the idea was to use a facial recognition algorithm with seven years' worth of jail system digital images to help positively identify individuals who might be giving fictitious names or who could not provide identification. From its inception, staff photographed everyone brought into the county jail at the sally port and compared their images to those already in the database.

"Shortly after we went live, the patrol deputies pointed out that if they pull someone over who is playing the 'name game' and doesn't have a driver's license, they have to decide if there is justification for bringing that person in for fingerprinting," Main says. "They thought it would be great to be able to take an image on the street and get results back."

Pinellas County began phasing that capability into patrol cars in 2004. By 2009, deputies made 496 arrests that could be directly attributed to identification made by the facial recognition technology and confirmed another 485 identities that did not require arrest, according to Systems Analyst Scott McCallum.

"The premise was to keep it short and simple for the deputy," Main says. "We didn't want them on the side of the street making extensive clicks and opening windows, so we worked with the vendor to completely automate the process. It's all pretty much hands-off; the deputy can keep an eye on the suspect while the computer does the work. However, if it brings up several potential matches, then the deputy does have to do some work to see if there is more information available, such as scars, marks and tattoos."

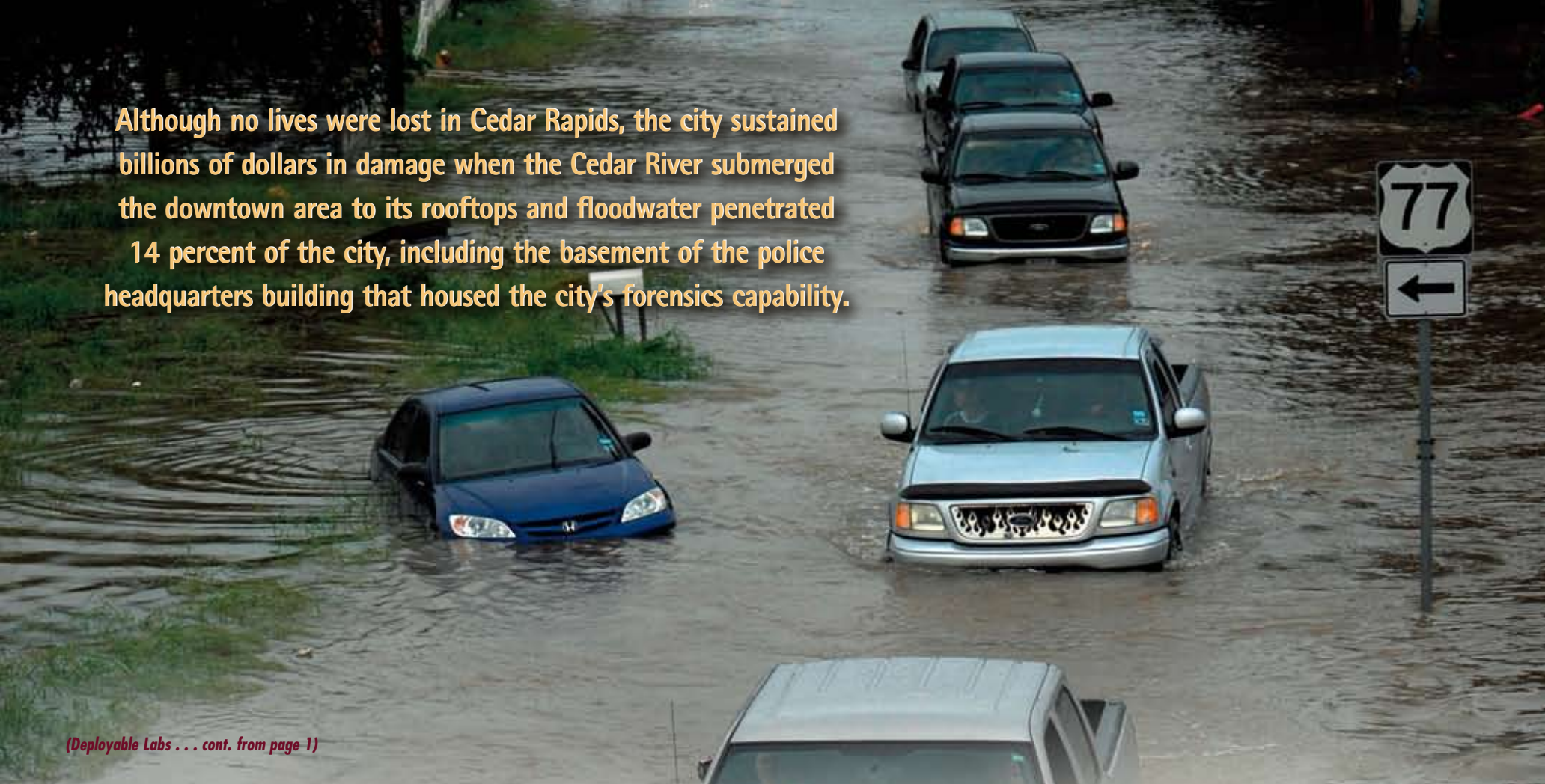
The system also benefits the county's correctional services, Main says, by ensuring the deputies know exactly who they are dealing with, not only with regard to identity, but also past history, including violent tendencies, chemical dependency issues and medical conditions.

These benefits began with the system developed using the original COPS grant, which went toward initial development. The county has since obtained additional funding to expand the system to 14 major metropolitan counties throughout Florida, and recently initiated a pilot project with the Florida Department of Motor Vehicles. The partnerships enable Pinellas County to search the other counties' databases, and vice versa.

"The more images you get, the greater chance you have of making a match," Main says.

Although the Florida system has expanded about as far as the licensing agreement will allow, other states and jurisdictions can purchase their own licenses from the same vendor and use them to establish their own compatible systems that use the same binary algorithm. Main says that agencies in both South Carolina and West Virginia have expressed interest in setting up similar programs. When these other systems come online, they will be able to transmit images back and forth to Pinellas County and perform reciprocal searches for each other. Even without compatible interfaces between other agencies, Pinellas County provides mutual aid and performs searches of its system for outside requests. For example, a recent request from the South Carolina Fusion Center resulted in a positive ID for a man who had been using numerous driver's licenses with different aliases.

For more information on the Pinellas County facial recognition project, contact Capt. Jim Main at (727) 582-6339 or e-mail jmain@pcsonet.



Although no lives were lost in Cedar Rapids, the city sustained billions of dollars in damage when the Cedar River submerged the downtown area to its rooftops and floodwater penetrated 14 percent of the city, including the basement of the police headquarters building that housed the city's forensics capability.

(Deployable Labs . . . cont. from page 1)

Cedar Rapids Deployment

Three years later, with units now available, the CoE had a chance to put Lothridge's plan to the test in Cedar Rapids, Iowa, where the media dubbed the massive flooding of June 2008 "the Midwest's Katrina." Although no lives were lost in Cedar Rapids, the city sustained billions of dollars in damage when the Cedar River submerged the downtown area to its rooftops and floodwater penetrated 14 percent of the city, including the basement of the police headquarters building that housed the city's forensics capability. The lab took on approximately eight feet of water and as the waters receded, the city's forensic technicians found themselves working in an unheated maintenance garage.

Sgt. Joe Clark of the Cedar Rapids Police Department drew the task of finding a better solution: "Even though we had suffered through a flood, we still had to follow the rules of the court and evidence collection procedures. The loan allowed us to operate in a professional manner during the interim period."

Clark started by calling vendors, contemplating trailers, mobile homes and other solutions as ways to provide extra space. Several companies said they could build him a mobile laboratory, but it would take six months and cost approximately $250,000.

"I was looking more for something we could rent. I called the home office of the International Association for Identification [a professional organization for crime scene investigators] and Executive Director Joe Polski said, 'I know just what you need to do, call Kevin Lothridge in Florida and they'll let you borrow one for free,' " Clark says. After visiting NFSTC to take a look at the labs in action, Cedar Rapids was in.

"The city is in pretty tough financial times, like all cities are, but on top of normal economic problems, we have hundreds of millions in flood damage to deal with," he adds. "I know that $250,000 to $300,000 for a lab doesn't sound like a lot, but this really made a difference to us. For a few thousand dollars paid to a trucking company, we were able to have a crime lab for more than a year and that quarter-million could be spent on essential services within the city."

Clark says the lab doesn't look very big from the outside, but it held all the lab equipment Cedar Rapids needed. "It has its own generator, which we used for a time until we could get it hooked up to our generator. I looked at how staff configured the labs they were using for testing and training at NFSTC and it gave me some ideas about setup."

NFTSC uses ductless chemical vent hoods with filters to remove processing fumes, eliminating the need to vent them outside, and places equipment on wheeled carts that could move around the lab. "If we get flooded again, we can unplug things and take them away and reconstitute the lab somewhere else."

Cedar Rapids used the deployable unit for slightly more than a year before returning to its new facilities in December 2009.

"They were very helpful, and I think we helped them a little bit too," Clark says. "Since the concept originated in Iraq, they had real nice air conditioning but the heating and the insulation didn't quite hold up to 25-below Iowa winters. We had to add space heaters, which sometimes played havoc with how much equipment could still be plugged into the generator while we kept warm. I think we gave them some feedback that helped improve the next generation."

Michigan State Police Deployment

The Michigan State Police also provided feedback during their use of two deployable labs, prompted in this case not by a natural disaster, but by another problem all too familiar to many law enforcement agencies in these economic times: budget cuts. David Stephens, director of the lab in Marquette, the only state police forensics laboratory located in the state's Upper Peninsula, says his lab had become targeted for possible closure despite serving 30 percent of the state's geographic area. (The Upper Peninsula has a lower population rate than the rest of the state).

To compound matters further, as the future of the lab remained in doubt, the facility lost its lease and needed to locate elsewhere. The lab presently is funded through Sept. 30, 2010, and continues to use the deployable facilities while searching for a site to lease. Stephens says he anticipates working with the office of U.S. Senator Carl Levin of Michigan in spring 2010 about obtaining additional federal funding.

Stephens says the deployable labs (one for latent print processing, one for firearms processing) are housed inside a heated garage, which helped alleviate some of the heating problems faced by Cedar Rapids. Like his counterparts in Iowa, Stephens also is impressed by the ductless fume hood.

"That's really quite nice," he says. "Hoods can be problematic in a lab. The ones we had at the old site were quite expensive to install and operate. The ductless hoods on the carts that can roll around save both time and money."

The Michigan State Police learned about the program through an NFSTC presentation at a conference and realized it could help provide a short-term solution to their problem while they wait to learn if the lab will remain open.

"We can have them for up to 18 months," Stephens says. "We've applied for some recovery monies to build a new forensics lab, and by using the deployable labs, if we get the grant, we don't have to use any of it to renovate an existing building to use while the new one is built. Renovations can be expensive and it doesn't make sense to do them on a temporary timeline."

There is also a possibility that the state could continue to fund the lab, but Stephens says that Michigan is facing a 15-percent unemployment rate and a corresponding budget shortfall due to lost revenues.

"This is a difficult time for law enforcement, for any public safety department as far as providing the same services, let alone advancing services."

For more information on the deployable forensic labs, contact the Forensic Technologies Center of Excellence, in care of the National Forensic Science Technology Center, at (727) 549-6067, or e-mail info@nfstc.org. The deployable lab program has won the August Vollmer Excellence in Forensic Science Award from the International Association of Chiefs of Police.

Agreement Fosters Lab Development

In August 2009, Acting Assistant Attorney General Laurie Robinson and Acting National Institute of Justice (NIJ) Director Kristina Rose signed a memorandum of agreement (MOA) between the Office of Justice Programs and the Defense Threat Reduction Agency (DTRA). This agreement leverages the capabilities, expertise and as applicable, technology development activities of DTRA to help meet forensic and law enforcement practitioner technology needs, consistent with the authorities of NIJ. The agreement encompasses collaborative activities addressing DTRA's state-of-the-art mobile forensic laboratory. Through this MOA, DTRA will loan six mobile forensic laboratory shelters, equipment and supplies to NIJ to support state and local law enforcement and forensic activities. The mobile forensic laboratories will be operated and maintained by NIJ's Forensic Technologies Center of Excellence through the National Forensic Science Technology Center.

BOMB SQUADS: Local Preparedness for Global Problems

Faced with a terrorist movement that went global several years ago, bomb squad commanders around the world have come to realize that the days of localized threats are over. In response, several agencies joined to host an Improvised Explosive Device Defeat Commanders Summit in Denver, Colo. Twenty-five U.S. bomb squad commanders and 10 of their non-U.S. counterparts who participate in bilateral research and development (R&D) programs with U.S. agencies attended the event on Sept. 23-25, 2009.

The event was hosted by the National Institute of Justice, the U.S. Department of Homeland Security's Science and Technology Directorate, the Combating Terrorism Technology Support Office-Technical Support Working Group, the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the National Bomb Squad Commanders Advisory Board (NBSCAB) and NIJ's Weapons and Protective Systems Technologies Center of Excellence.

Participants brought with them examples of the technical and tactical challenges they have faced and the solutions they have developed so that attendees could share the knowledge required to defeat this global issue. Their efforts will produce a compilation of the challenges and solutions shared plus strategy-related recommendations brought out during breakout sessions focusing on vehicle-borne improvised explosive devices (VBIEDs), person-borne improvised explosive devices (PBIEDs), homemade explosives, training and intelligence.

"This summit was truly the first step in bringing together a worldwide bomb technician community of practice," says Edwin Bundy of the Technical Support Working Group. "I sincerely hope that this is the first of many such summits, and there is little doubt that the bonds formed here will strengthen not only the U.S., but also the international effort to combat terrorist use of explosives."

NBSCAB declared in 2007 that VBIEDs pose the greatest technological challenge to bomb squads. The size, mobility, complexity and magnitude of VBIED explosions take this threat out of the realm of normal bomb squad response tools, which have evolved over the years to deal with briefcases, backpacks, pipe bombs and illegal fireworks. During this summit, the group discussed the advances needed in robotic technologies to be effective against VBIEDs. In presentations and breakout sessions, the group shared experiences, challenges and potential solutions to deal with both diagnostic and defeat issues for VBIEDs.

"There was a shared recognition among the group that the VBIED challenges are real," says Jim Hansen, NBSCAB chairman. "Nobody has the complete answer yet on either the diagnostic front or the defeat front. Ideas for both of these areas were discussed this week, but nobody has developed the magic bullet for either of them.

"Even if you defeat the firing mechanism of the bomb, your problems are not over when dealing with homemade explosives in large quantities, which present their own set of handling and disposal hazards. There was an admission among the group that VBIED defeat technologies are not developed to the levels we need, and that our fallback is to train on the tools we have, with emphasis toward improving the hands-on skills in life threatening situations," he says.

The PBIED threat brings with it the challenge of dealing with a human who is attached, in whatever way, to the IED. Whether alive or dead, whether victim or criminal, a PBIED complicates the operational response procedures for the bomb squad and poses daunting technological and tactical challenges.

Some of the non-U.S. participants at the conference who have extensive experience in dealing with suicide bombers shared their lessons learned. Discussion revealed the wide range of skills and technologies needed to deal with PBIEDs, including interaction with tactical teams in hostile takeover situations, hands-on device defeat in hostage scenarios and robotic manipulation of incapacitated suicide bombers whose devices may have malfunctioned.

The manufacture and use of homemade explosives (HME) has been on the rise in the past decade, with the number of chemical variations growing in geometric proportions and the sensitivity levels of each pressing safe-handling limits for bomb technicians. Some presentations included case studies in which bomb squads had to deal with unknown sensitive explosive mixtures. Other presentations dealt with a recent sharp rise in information available on the Internet on how to manufacture HME. In breakout sessions, the group made several valuable recommendations for potential R&D efforts.

In the conference final wrap-up, the group concluded that bomb squads in the various countries face different threats and threat levels, leading to differences in experiences and solution sets, and deal with different governmental structures, leading to differences in policies, equipment and training program structures. However, there are similarities as well:

- A fundamental concern for public safety leads to similarities in priorities.
- The global scale of terrorism makes any threat everyone's threat.
- There is a universal understanding that technological challenges are shared by all and shared technology solutions pay the greatest dividends.
- The skills needed for the bomb technician's task are increasing on a geometric scale.

Participants in the event recognized that international standards at a professional level can be achieved. While basic training is program-centric and tends to become its own standard operating procedure, specialty training programs evolve from the fringe and can best be coordinated through professional standards validated by a core training program. Meaningful standards may be possible by starting with specialty areas and working back toward the center. Participants also recognized that the challenges bomb squad commanders face are increasing at a daunting pace and there is a clear need for training development at the commander level.

For more information on the conference and the availability of the report, contact the Weapons and Protective Systems Technologies Center of Excellence at (800) 248-2742.

FIRST RESPONDER CREDENTIALS

Expedite Access

During an emergency involving multiple jurisdictions, having a trusted means to rapidly identify law enforcement and other responders is essential. An evolving federal credentialing program is providing that capability, along with other uses.

The technology used in the credentials, known as First Responder Authentication Credentials (FRACs), provides trusted and electronically validated identification, interoperable across federal, state and local jurisdictions. Identity authentication checks are made easily at an emergency scene, where a handheld reader device or a laptop in a law enforcement cruiser can verify the individual's identity.

The U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) have been working with state agencies for several years in a series of pilot demonstrations to test various emergency scenarios using the credentials. The goal is to encourage adoption and operational use of high assurance authentication credentials nationwide.

The FRAC effort is part of a broader enterprise strategy to leverage investments, innovations and enhanced capabilities of Personal Identity Verification (PIV) credentials being issued to all federal employees and government contractors. In 2004, Homeland Security Presidential Directive 12 (HSPD 12) mandated new standards for secure and reliable personal identification for federal employees and contractors. The credentials are to be used for accessing federal buildings and computers. The National Institute of Standards and Technology issued the standard for credentialing employee identification credentials (Federal Information Processing Standard (FIPS) 201-1).

FRACs use the same technology as PIV credentials. They contain encrypted identification information, including name, agency and two fingerprints. A credential holder has a personal identification number (PIN) that must be entered into a credential reader to allow access to the credential's information.

"It allows incident commanders to make a better, informed decision about who to allow in," says Thomas Lockwood, senior advisor for the DHS Screening Coordination Office. "You have a very high level of assurance that the person is who he/she claims to be."

The scenario demonstrations using FRACs have included federal, state and local emergency response officials as well as utility companies and transportation agencies. Reaction from emergency response officials who have participated in demonstrations has been positive, says Craig Wilson, Federal and Mutual Aid Emergency Response Official Coordinator for the FEMA Office of National Capital Region Coordination.

"When asked if the technology gave law enforcement officials the ability to make an informed decision for access permission, the resounding answer from everyone has been yes," Wilson says.

Colorado is among states that have participated in pilot programs. Micheline Casey, director of identity management in the Colorado Governor's Office of Information Technology, says they plan to issue between 10,000 and 15,000 FRACs over the next two years in the north central region, which includes the Denver metropolitan area.

"I think that, overall, people are really enthusiastic," Ms. Casey says. "We are a rural state with most of the population in the Denver metropolitan area, so people tend to go across county boundaries to help each other out, and they don't always know everyone who shows up."

Colorado is looking at a variety of ways to apply the technology beyond use during a major incident; for example, access to buildings including jails and courthouses and access to computer systems and networks.

"FEMA is using the technology for ultimate worst case scenarios, but identity management is done the same way whether it's getting into a building, bank, your car or a disaster scene," Wilson says. "The key is to get everyone moving in the same direction. We are truly achieving robust interoperability that can be trusted."

Progress continues to be made at the federal HSPD-12 level. The General Services Administration's Managed Services Office (MSO) provides credentialing services to over 70 federal agencies, including the U.S. Department of Justice, according to Raymond Kimble of Excella Consulting, which supports the MSO. To date, approximately 400,000 people have been issued credentials through the MSO for identification and building access, and that number will eventually grow to 800,000 people.

For more information, contact Stephen Duncan, branch chief, GSA HSPD-12 Managed Services Office, at (703) 605-3492.

The goal is to encourage adoption and operational use of high assurance authentication credentials nationwide.

Social Networking for Law Enforcement

Searching for ways to improve community relations and expedite information to the public, law enforcement agencies are turning to social networking sites.

Police departments use the sites to rapidly communicate directly to citizens, providing such information as suspect descriptions, crime alerts, road closings, missing child and person alerts, dangerous weather conditions and traffic accidents.

People voluntarily reveal details of their lives on social networking sites, which can serve law enforcement well. Sites such as Facebook® and MySpace™ can be used by law enforcement to obtain information about suspects, for example, involvement in gang activity. Photos or videos of suspects can be posted as well. Sites such as YouTube™ are being used to foster police recruitment.

Citizen subscribers to sites such as Twitter™ and Nixle can automatically receive police department information via text message, e-mail or by logging on to those sites.

Law enforcement agencies of all sizes are using the technology. Described below is how three diverse police departments — Baltimore and Mt. Rainier in Maryland and Modesto, Calif. — are using the sites to their advantage.

For descriptions of various networking sites and useful Web sites, see the sidebar, "Networking Sampler."

Baltimore, Md.

The Baltimore Police Department, with 4,000 civilian and sworn personnel, is the eighth largest municipal police force in the United States, serving a city population of 641,000. The department is embracing the use of social networking sites in a variety of ways to enhance information flow and community relations.

The department began using Facebook® and Twitter™ in March 2009, and is experimenting with Nixle. Baltimore has nine police districts and has implemented Nixle in the southeastern and northwestern districts. The goal is to implement Nixle citywide in addition to Facebook® and Twitter™, according to Anthony Guglielmi, director of public affairs for the department.

"Part of the police commissioner's crime fighting plan includes community engagement and involving the community, and part of that is sharing of information," Guglielmi says. "Residents have a right to know if a homicide or a violent crime has occurred in their neighborhood when it occurs, and not have to wait. That's what we use Twitter™ and Facebook® for. We use them as an extension of the local news media because the media can't cover everything that happens and involves the department."

Baltimore also uses YouTube™ to foster police recruitment. An in-house video production unit rides along with officers on patrol and records police academy graduations, then edits the results and prepares a video package to post to YouTube™.

Guglielmi says Facebook® is useful for posting information on wanted suspects, department news and links to video. Police have received photos of accident scenes via Facebook®. Also, officers have their own Facebook® pages, allowing the community to interact with individual officers.

"It's about getting people engaged," he says. "What we really like about [social networking sites] is they engage people in a dialog to talk about crime. If people are talking about it and keeping abreast of what is going on, they're going to hopefully take part in crime fighting through partnering with the police and participating in community groups. Even things like littering that affect life in a community — we want to solicit feedback as much as we can."

Although Baltimore uses Twitter™ to inform the public, the department does not encourage users to submit tips through Twitter™ because of security concerns; anyone could view the information. If police are seeking information, they will include a contact number with the post. The department is working on establishing a secure text message tipline so people can send text messages from Twitter™ that no one else can view. Also, given that the department has almost 4,000 followers on Twitter™, it would be impossible for staff to keep up a constant two-way discussion on everything the department posts, and so the department uses it as a broadcasting tool rather than a discussion tool.

One challenge is verifying and maintaining accuracy of information. The department receives large amounts of information, which must be verified before notifying the public on Twitter™ or another site. For example, an incident call came in as a shooting, which turned out to be an individual who had fallen on the sidewalk. "You don't want to put out information that causes unnecessary concern," Guglielmi says. Once an event is confirmed, police can use Twitter™ to notify the public and provide running updates as a situation evolves.

Police need to ensure that information they distribute is accurate and head off false information that may circulate in the community as an event unfolds. Guglielmi explains that during one hostage barricade situation, citizens were communicating live on Twitter™.

"Officers used tear gas and residents were twittering that it was gunshots, which created hysteria, so we need to be vigilant on the police side and constantly update the Twitter™ page to make sure that the information and the chatter is accurate. We don't want bad information getting out there and people panicking."

Keeping the sites up to date requires manpower. Officers ensure Twitter™ and Facebook® are updated within 20 minutes after a confirmed major incident occurs. Officers can also post to Twitter™ and Facebook® from their BlackBerrys.

"It's as close to realtime as possible," Guglielmi says. "It's been an incredibly successful tool for us. The community seems to really like it. They are really good tools for us and have a lot of possibilities. I think in two years from now it will be a standard for law enforcement."

Nixle offers a secure communication platform tailored for police departments and municipalities. User applicants have to go through a vetting process before being accepted. Also, Nixle can target an alert to a specific geographic area or neighborhood.

In May 2009 police received a solid lead on a homicide via Facebook®. The tip was originally posted as a "wall post" that anyone could see, but police quickly removed it. "We don't want to show our hands before an arrest is made and we never would want to increase the exposure or risk for people providing the information," Guglielmi says."

For more information about the Baltimore Police Department's use of social networking sites, contact Anthony Guglielmi at (410) 396-2012 or e-mail Anthony.guglielmi@baltimorepolice.org.

Modesto, Calif.

Use of social networking sites boosts police/citizen relationships and flow of information to the public, but overuse can result in too much of a good thing, cautions Sgt. Brian Findlen, public information officer for the Modesto Police Department.

The department has about 370 total personnel, 250 of which are sworn officers. Serving a population of 205,000, the department uses Nixle and Twitter™ to communicate with the public.

"It has to be necessary, pertinent information that makes a difference in people's lives at that point in time," Findlen says. "We need to be careful because if we provide information to people that is not pertinent, we can cause them to unsubscribe. We need to choose the information carefully and not just put it out because we have the ability to do so.

"You can overdo it and blast out too much information. You can annoy people to the point that they turn you off, and that is counterproductive."

The department began using Twitter™ in 2008 and Nixle in 2009. The department uses Nixle as its primary site, automatically posting crime and public safety information to Twitter™ through an interface with Nixle. Nixle allows the posting of more lengthy information. Citizens who subscribe to Twitter™ will be routed to Nixle if they choose to read the full details. A checkbox on the Nixle screen allows a portion of the message to be posted to the department's Twitter™ site. Twitter™ subscribers can view the message, which includes a link to Nixle if the user chooses to read the full text.

Twitter™ has had at least one instance of people setting up a bogus police site. Findlen says Nixle, which is tailored specifically for law enforcement and municipalities, is more secure. It has an extensive verification process for site applicants and allows targeting of information to specific geographic areas, from a quarter-mile radius of an incident to as far as 20 miles.

"It's exactly what we needed," Findlen says. "We can put as much or as little information as we want and can tailor it to specific neighborhoods, the entire city or the county, so we know the information is hitting who it is supposed to hit."

Nixle has templates for posting different types of information, for example, missing persons. "It makes it so simple, anybody without training could use Nixle and post a message and understand it," he says.

"Since Twitter™ generates the user base quicker, my suggestion to law enforcement agencies is that if they are comfortable creating a Twitter™ account, they create one along with a Nixle account, but enter information into Nixle, which can download to Twitter™." The department's Twitter™ site has more than 1,500 followers.

In late August 2009, police chased a vehicle containing suspects in a double homicide. The armed suspects abandoned the vehicle and fled on foot. During the subsequent manhunt in a residential neighborhood, Findlen used Twitter™ to keep citizens updated through when arrests were made and the neighborhood police perimeter lifted.

"We were dealing with a serious situation, the public was in danger and we needed them to have information. It was an avenue through which at least some people were getting the information.

"I find use of the sites to be a positive experience. There is no maintenance on our end. It's an easy means to distribute information from our patrol cars or laptop computers. We can put information out with no delay, with no middleman at no cost," Findlen says.

For more information about the Modesto Police Department's use of social networking sites, contact Sgt. Brian Findlen at (209) 652-1386 or e-mail findlenb@modestopd.com.

Mt. Rainier, Md.

Even small law enforcement agencies are implementing blogging and social networking technology as a way to better connect with the communities they serve.

Michael E. Scott, chief of the 17-officer Mt. Rainier Police Department, runs the department blog himself, updating it daily for the past three years to keep the community up to date on criminal activity.

"It's there to provide information to the community," Scott says. "It helps keep the public informed about what is going on and it gives them the opportunity to respond in cases where they have information about the crime or the incident.

"It also helps dispel a lot of rumors and myths and tells people what really happened. They get the facts before they have to ask."

Everything posted to the blog cross-publishes to the Mt. Rainier Yahoo® group, and discussion comes through the Yahoo group. Scott continues publishing the blog because out-of-state people read it.

Mt. Rainier, with an approximate population of 10,000, borders Washington, D.C. "In Mt. Rainier, the police chief can get directly involved. People can pick up the phone and call the chief of police here. They get to know the police officers."

The department is registered with Twitter™, but rarely posts to it, and plans to use Nixle. Scott notes that Nixle's servers are housed on NLETS (International Justice and Public Safety Network), a secure information sharing system for state and local law enforcement agencies. When police departments publish on Nixle, the public knows the information comes from police. Nixle is a one-way service; citizens cannot post comments on it. It's used to push information out to the public.

"I believe that we have to use every tool in the tool box to get information out to the public," Scott says. "It gets emergency information out quickly, dispels myths and keeps the public informed. The more information is released ahead of time, the better the relationships between police and the community."

In addition to garnering citizen tips about crimes, the blog has helped police in forming neighborhood watch groups. "The value is community relations, and the information that flows out breaks down the traditional barriers between police and the community and gives police a face to the community."

For more information about the Mt. Rainier Police Department's use of social networking sites, contact Chief Michael E. Scott, at (301) 985-6580 or mscott@mountrainiermd.org.

(See Networking Sampler, page 12)

READY TO RUMBLE
MOCK PRISON RIOT 2010

Spring is coming. Time for a riot.

Each year in May since 1997, the Mock Prison Riot™ is held at the former state penitentiary in Moundsville, W. Va. Hosted by the Office of Justice Programs' National Institute of Justice (NIJ) and the West Virginia High Technology Consortium Foundation, the riot is used to showcase and evaluate emerging and existing law enforcement and corrections technologies.

The event has grown from a one-day event to a four-day, comprehensive law enforcement and corrections tactical and technology experience that includes more than 40,000 square feet of exhibit space, training scenarios, technology demonstrations, technology assessments and evaluations, certification workshops and a skills competition.

Law enforcement and corrections practitioners can touch, see and actually deploy new and emerging technologies under simulated "real-world" conditions. Practitioners can also wander through a technology showcase of exhibits and learn more about the technologies used in the numerous training scenarios.

The event draws corrections and law enforcement practitioners from across the U.S. and around the world. In 2009, 1,142 people attended from 43 states and 13 foreign countries. One hundred technologies were showcased.

Participants provide feedback on technology through formal assessment reports and through conversations in the showcase area and on the grounds after training events. On-the-spot feedback and question-and-answer sessions are encouraged.

All technologies are carefully evaluated by staff, with special emphasis placed on those technologies identified as high priority by NIJ, ensuring that the Mock Prison Riot™ offers the chance to experience and evaluate the most appropriate technologies under realistic conditions.

This year, participants have a new tool at their disposal to assist teams in planning and executing technology training scenarios. Planners can download and install a 3-dimensional model of the penitentiary to their computers from http://www.mockprisonriot.org.

"A primary factor that contributes to the level of realism at the Mock Prison Riot is the ability of exhibitors and law enforcement and corrections practitioners to conduct reconnaissance, planning and preparation for the areas where they will demonstrate and deploy technologies," says Sharon Goudy, one of the project managers for the riot. "The ability to preview locations for technology demonstration and deployment via a 3D, interactive means ensures that the most appropriate technologies and corresponding areas of operation are selected under any given circumstances."

Goudy adds that the ability to virtually coordinate and select the most appropriate technologies and locations for scenarios, demonstrations and assessments ahead of time ensures the most accurate practitioner feedback, which is critical to the technology development process.

Minimum system requirements to run the 3D program:

- Windows XP or Vista.
- Intel or AMD Processor @ 1 Ghz.
- 256 MB RAM (1GB recommended for Vista).
- 100 percent DirectX compatible video card with 128 MB video RAM required and Pixel Shader 3.0 support DirectX 9.0c.

Recommended system requirements:

- Windows XP or Vista with latest service packs installed.
- Dual-Core Intel or AMD processor @ 2.0 GHZ or better.
- 2 GB RAM.
- 100 percent DirectX compatible ATI or Nvidia based video card with 256 MB or more video RAM and Pixel Shader 3.0 support DirectX 9.0c.

Users of the 3D program will have virtual access to the dining hall, basement, infirmary, six cell blocks and a few other areas of the penitentiary.

The next Mock Prison Riot will be held May 2-5, 2010. For more information or to register, visit http://www.mockprisonriot.org or contact Cindy Barone or Sharon Goudy at (888) 306-5382.

NCJRS
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 a range of services and resources, balancing the information needs of the field with the technological means to receive and access support.

Access NCJRS Online

The NCJRS Web site showcases the latest criminal and juvenile justice and drug policy information. Take advantage of:

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

Join the Information Network

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

JUSTINFO. A biweekly electronic newsletter that includes links to full text publications, notices of upcoming trainings, funding announcements and other resources.

E-mail notifications. Periodic messages about new resources that match your specific areas of interest.

RSS feed. Receive notices of NCJRS homepage updates or embed the feed on your Web site to pull content directly from our home page.

Contact NCJRS

Web: http://www.ncjrs.gov

Phone: (800) 851-3420
(Monday – Friday,
10 a.m. to 6 p.m. EST)

Fax: (301) 519-5212

Mail: NCJRS, P.O. Box 6000,
Rockville, MD 20849-6000

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. 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; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

Let Techbeat Help you find the solution

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 pro vide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact (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 Winter 2010 issue of *TechBeat,* published by the National Law Enforcement and Corrections Technology Center, a program of the Office of Justice Programs' 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 Govern ment Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; the APEX 2001 Award of Excellence for Magazines and Newspapers–Printed; the APEX 2006 Award of Excellence Newsletters Print; and a 2009 Award of Excellence, External Magazine, from the National Association of Government Communicators.

Photo Credits: Photos used in this issue of *TechBeat* ©2010 Shutterstock; Arresting Images; Pinellas County Sheriff s Office; Corbis Images; iStock; and Sam Brown, Lockheed Martin.

Flickr® logo reproduced with permission of Yahoo! Inc. ©2010 Yahoo Inc. FLICKR® and the FLICKR® logo are registered trademarks of Yahoo! Inc.

Staff: Interim Managing Editor, Lance Miller; Editor, Michele Coppola; Lead Writer, Becky Lewis; Graphic Designers, Tina Kramer and John Graziano.

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 Web sites.

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 Web sites.

TECH shorts
Technology News Summary

TECHshorts is a sampling of the technology projects, programs and initiatives being conducted by the Office of Justice Programs' National Institute of Justice (NIJ) and the centers and criminal justice technology Centers of Excellence (CoEs) that constitute its National Law Enforcement and Corrections Technology Center (NLECTC) system. If you would like additional information concerning any of the following TECHshorts, please refer to the specific point-of-contact information that is included at the end of each entry.

In addition to TECHshorts, an online, biweekly technology news summary containing articles relating to technology developments in public safety that have appeared in newspapers, newsmagazines and trade and professional journals is available through the NLECTC system's Web site, JUSTNET, at http://www.justnet.org. This service, the *Law Enforcement and Corrections Technology News Summary,* also is available through an electronic e-mail list, *JUSTNETNews.* Every other week, subscribers to *JUSTNETNews* receive the news summary directly via e-mail. To subscribe to *JUSTNETNews,* e-mail your request to asknlectc@nlectc.org or call (800) 248-2742.

Note: The mentioning of specific manufacturers or products in TECHshorts does not constitute the endorsement of the U.S. Department of Justice, NIJ or the NLECTC system.

Annual Conference Spotlights Technology for Community Corrections

NLECTC-Rocky Mountain

With more than 5 million adults on probation or parole supervision, community corrections is a vital component of the criminal justice system. That population will only increase as many states explore plans to release inmates from facilities into community supervision as a cost-saving measure. Thus, it is now more important than ever for agencies to look to technology for ways to provide services in a more effective and efficient manner. To help in this endeavor, the National Law Enforcement and Corrections Technology Center-Rocky Mountain puts on an Innovative Technologies for Community Corrections Conference. This event, which began in 2000, provides a showcase for agencies looking for ideas, resources and models to help them use technology to enhance mission performance.

In June 2009, the 10th annual conference took place in San Diego, attracting more than 200 practitioners from across the country. Conference presentations covered a variety of technology applications in the general areas of electronic monitoring, information technology, computer monitoring, drug and alcohol testing, and risk assessment. One presentation of particular interest, delivered by a representative of the Kentucky Division of Probation and Parole, discussed that agency's monitoring of social networking tools such as Facebook® and MySpace™ as a means of investigating offender activities and supporting fugitive apprehension efforts. Another presentation, delivered by NLECTC-Rocky Mountain staff, focused on methods of testing GPS technology for accuracy and reliability. That presentation included protocols that an agency can use to evaluate different products to determine how they might work in a particular location.

For further information on the upcoming 2010 Innovative Technologies for Community Corrections Conference, visit www.justnet.org or e-mail contact Joe Russo at jrusso@du.edu.

Computer Forensic Software Automates Macintosh Investigations

National Institute of Justice

Architecture Technology Corporation, creator of P2P Marshal (see "Tool Helps Automate, Expedite Cybercrime Probes," Fall 2009 *TechBeat*) has used a different NIJ grant to develop Mac Marshal™, an automated forensic software package that extracts more and better information from Mac systems by using Mac tools to see Mac files the way Macs see them. Like P2P Marshal, law enforcement agencies can download Mac Marshal at no charge.

The forensic software can scan a Mac disk image and automatically detect Mac, Windows and other operating systems and virtual machine images. Its analysis tools can extract Mac OS X-specific forensic evidence (e.g., data left by Apple's Mail, Safari, Address Book, iChat). Mac Marshal maintains a detailed log file of all activities it performs, as required by forensic best practices.

According to its developers, Mac Marshal features include the ability to:

- Examine Mac OS X and dual-boot disk images.
- Analyze configuration and log files from common OS X applications.
- Perform rapid searches (using Spotlight metadata).
- Gather comprehensive machine usage information.
- List detailed information about every iPod and iPhone ever connected to it.
- Detect and show VMWare, Parallels and Virtual Box virtual machine images.
- Detect and analyze FileVault-encrypted user directories.
- Support dd, EnCase, FTK, AFF and Apple disk images.
- Maintain an audit trail and generate detailed reports in RTF, PDF and HTML formats.

In order to run Mac Marshal, an investigator needs a Mac OS X 10.4, 10.5 or 10.6 analysis machine and 50 MB free disk space.

For more information about Mac Marshal, visit http://www.MacMarshal.com.

NIST Guidelines Help Officers Link Mobile and Stationary Biometric ID Systems

National Institute of Standards and Technology

In August 2009, the National Institute of Standards and Technology (NIST) published *Special Publication 500-280: Mobile ID Device Best Practice Recommendation Version 1,* which provides new best practices guidelines on the use of the next generation of portable biometric technology (Mobile ID) and how to best make it work with existing desktop systems. Researchers at NIST collected input from first responders, industry, the military and academia before developing the guidelines.

New mobile devices enable law enforcement professionals to collect biometric data anywhere using a handheld device. Information can then be wirelessly transmitted for near real-time comparison to watch lists and databases, allowing for possible on-scene confirmation of a suspect's identity. Mobile devices can also be used to ensure that only appropriate personnel have access to an incident site.

At the time the publication was released, NIST noted that although advances in the use of portable systems have been rapid, there are still limitations to consider to ensure interoperability with stationary systems. Most law enforcement applications currently require all 10 of an individual's fingerprints, for example, and using the large platens on desktop scanners, officers can scan all 10 fingers quickly in three steps (left hand, right hand and both thumbs together). However, most mobile devices have much smaller platens, making capture of all 10 fingerprints difficult. The NIST guidelines offer advice on using a two-fingers-at-a-time approach to quickly get the needed data.

Previous publications related to biometric devices had focused more on interoperability between different stationary and desktop systems.

Special Publication 500-280: Mobile ID Device Best Practice Recommendation Version 1 ***can be downloaded from http://fingerprint.nist.gov/mobileid/MobileID-BPRS-20090825-V100.pdf.***

FBI Suspends Hair Analysis for Cocaine

National Institute of Justice

The FBI laboratory at Quantico, Va., has suspended testing hair samples for cocaine for most cases because of research findings that suggest the drug can be externally absorbed into hair at higher levels than previously thought.

The suspension of testing is explained in a letter to the editor in the July/August 2009 issue of the *Journal of Analytical Toxicology.* The letter was written by Marc Lebeau and Madeline Montgomery of the Laboratory Division at Quantico. The FBI will continue to test the hair of children for cocaine in criminal cases.

The letter notes that in an NIJ research grant final report released in January 2009, *Analysis of Cocaine Analytes in Human Hair: Evaluation of Concentration Ratios in Different Hair Types, Cocaine Sources, Drug-User Populations, and Surface-Contaminated Specimens,* researchers Jeri Ropero-Miller and Peter Stout described several experiments to determine if the hair of chronic cocaine users could be distinguished from hair that was externally contaminated with cocaine hydrochloride. The findings of the report suggest that cocaine is incorporated into human hair through exterior contamination in concentrations similar to the amounts found in the hair of cocaine users.

Identification of cocaine in hair means an individual was exposed to cocaine. "What remains unclear," the letter says, "is if that exposure was from unknown contact, contact as part of the individual's occupation, exposure through being in a room while cocaine was being used, or if it is from personal use by the subject. Without a justifiable interpretation of positive cocaine findings in hair, our laboratory will decline to perform these examinations except for criminal cases involving children."

The letter noted that further research is needed to determine the best approach to differentiate ingestion of cocaine from external exposure.

***To view the NIJ research grant report,* Analysis of Cocaine Analytes in Human Hair: Evaluation of Concentration Ratios in Different Hair Types, Cocaine Sources, Drug-User Populations, and Surface-Contaminated**

Specimens, ***visit http://www.ncjrs.gov/pdffiles1/nij/grants/225531.pdf. To view the letter to the editor, visit http://www.jatox.com.***

High-Speed Pursuit Technology Study

Weapons and Protective Systems Technologies CoE

For the past year, researchers at the Weapons and Protective Systems Technologies Center of Excellence (WPSTC), located at Pennsylvania State University, have been studying ways to help law enforcement personnel by evaluating the techniques, tactics and technologies used to manage high-speed pursuits. Using databases of pursuit timelines, researchers at the Applied Research Laboratory and Larson Transportation Institute examined the relationship between pursuit management technologies and pursuit outcomes.

Findings indicate that tire deflation devices (TDDs) and the precision immobilization technique (PIT) maneuver account for the majority of recorded intervention tactics. In summer and fall 2009, WPSTC tested the three most common TDDs and evaluated vehicle dynamics during the use of the PIT maneuver. The TDD study compared effectiveness of tire deflation technology at various speeds, various deployment conditions and tire types. Also, as a result of findings by the Federal Law Enforcement Training Center (FLETC) related to the use of PIT against the electronic stability equipped (ESC) Dodge Charger, WPSTC plans to partner with FLETC to further evaluate the safety and effectiveness of the PIT maneuver against various conventional vehicles as well as those equipped with ESC systems.

WPSTC will publish the findings of both the TDD-attribute based evaluation and the PIT vehicle dynamics study later this winter and will also develop a free reference card with information on tire deflation rates, costs of devices and safety information to facilitate better informed procurement decisions on TDDs by individual agencies. In cooperation with FLETC, WPSTC plans to also publish a report on the effectiveness of PIT against conventional and ESC-equipped sedans and SUVs.

For more information, contact Mike Hendrickson at the Weapons and Protective Systems Technologies CoE at (814) 865-1289 or e-mail mxh181@psu.edu.

the NLECTC 'center system'

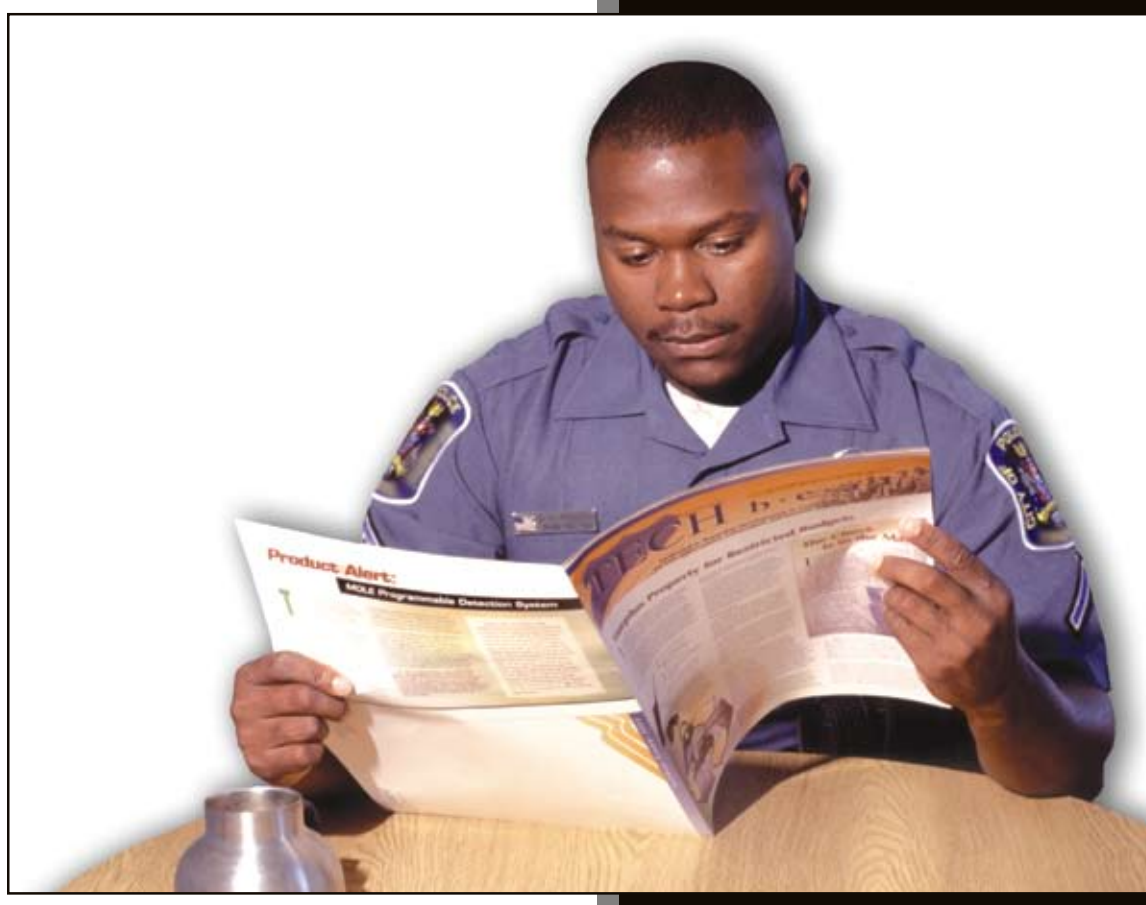
The National Law Enforcement and Corrections Technology Center (NLECTC) system supports the National Institute of Justice (NIJ) mission of providing objective, independent, evidence-based knowledge and tools to enhance the administration of justice and public safety.

The NLECTC system is an integrated network of centers and Centers of Excellence that offer free criminal justice technology outreach, demonstration, testing and evaluation assistance to law enforcement, corrections, courts, other criminal justice agencies and crime laboratories — large or small, rural or urban and along U.S. borders — in the implementation of current and emerging technologies.

The NLECTC system has been reorganized to make it more sustainable, efficient and effective in providing services to the criminal justice community.

Established in 1994 by the Office of Justice Programs' NIJ as part of its research, development, testing and evaluation initiatives, the NLECTC system serves as an "honest broker" resource for technology information and assistance and helps introduce technologies into practice within the criminal justice community. The mission of NLECTC is to support NIJ's research and development activities, support the transfer and implementation of technology into practice, assist in the development and dissemination of guidelines and technology standards, and provide technology assistance, information and support.

The NLECTC system seamlessly delivers its expertise to the nation's 19,000-plus police agencies; 50 state correctional systems; thousands of prisons, jails, and probation and parole departments; courts; and crime laboratories in a number of technology areas. These technology areas are supported by technology partners who provide the leveraging of unique science and engineering expertise. In addition, technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for NIJ's various technology focus areas and help to ensure that NIJ's activities focus on the real-world needs of public safety agencies.



Contact NLECTC for:

Technology Information

NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, product information databases, news summaries, meeting/conference reports, online videos and CD-ROMs. 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 Identification

The NLECTC system provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities and interoperability.

Technology Assistance

Our staff serves as proxy scientists and engineers. Areas of assistance include systems engineering and communications and information systems support (e.g., interoperability, propagation studies and vulnerability assessments).

Technology Implementation

We develop technology guides, best practices and other information resources that are frequently leveraged from hands–on assistance projects and made available to other agencies.

Property Acquisition

We help departments take advantage of surplus property programs that make federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Testing and Standards

We oversee the development of performance standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs and semiautomatic pistols is tested. 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.

Technology Demonstrations and Capacity Building

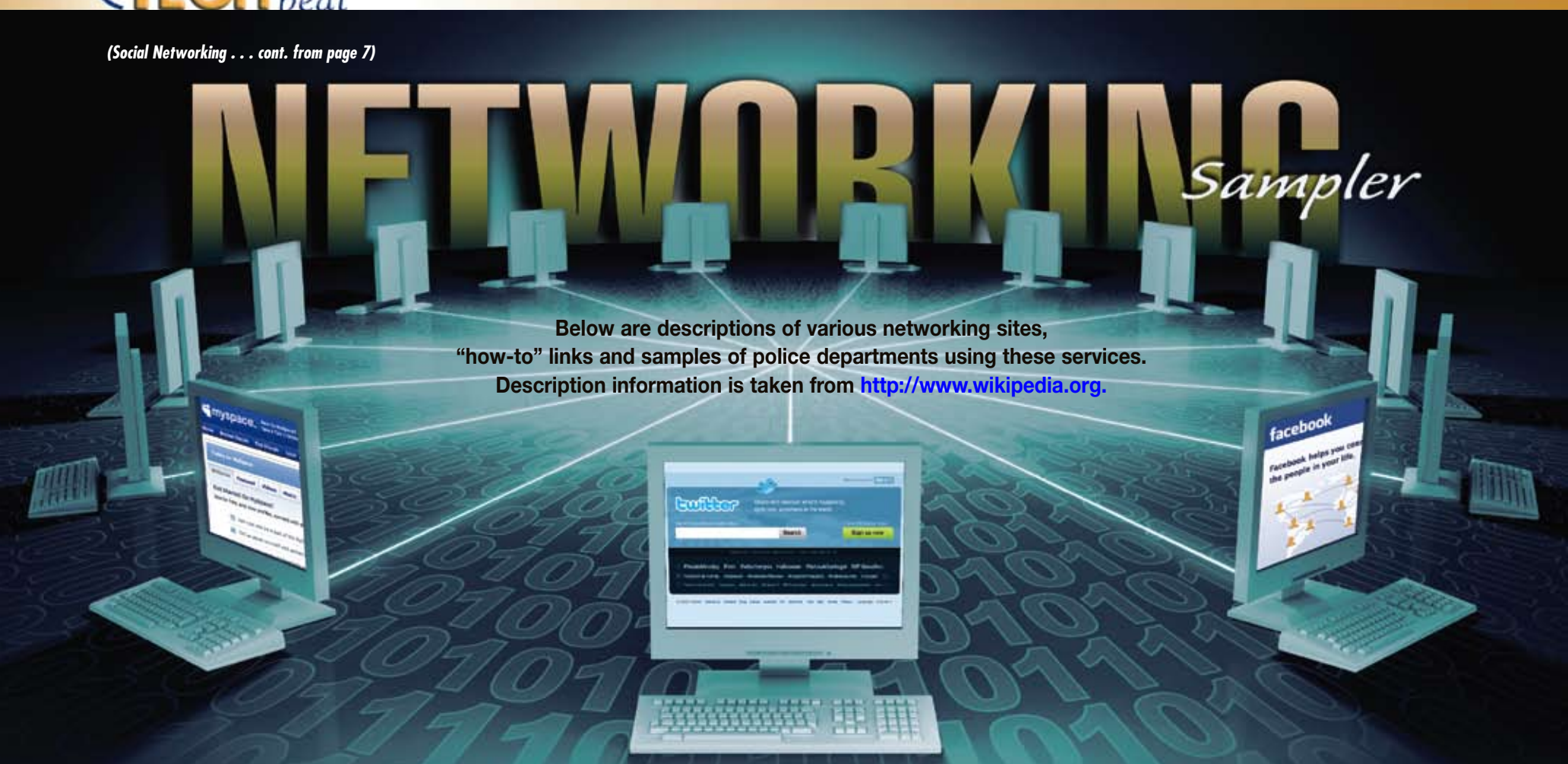
We introduce and demonstrate new and emerging technologies through special events, conferences and practical demonstrations such as the Mock Prison Riot™. We also provide hands-on training assistance for the latest technologies through workshops and software programs dealing with crime mapping, community corrections and critical incident management. In addition, on a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

NLECTC-National
2277 Research Blvd.
Rockville, MD 20850
(800) 248-2742 ■ asknlectc@nlectc.org
asknlectc@nlectc.org

National Law Enforcement and Corrections Technology Center
c/o ISTG Annapolis Junction Warehouse
9015 Junction Drive
Annapolis Junction, MD 20701

(Social Networking . . . cont. from page 7)

NETWORKING Sampler



Below are descriptions of various networking sites, "how-to" links and samples of police departments using these services. Description information is taken from http://www.wikipedia.org.

Twitter™. Twitter is a free social networking and micro-blogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers.

http://help.twitter.com/portal

http://twitter.com/BaltimorePolice

http://twitter.com/Boston_Police

http://twitter.com/portsmouthpd

How to Set Up a Twitter Account

http://www.twitip.com/how-to-set-up-a-twitter-account/

Nixle. Nixle is a community information service provid er and built exclusively to provide secure and reliable com munications. It is a secure service that connects municipal agencies and community organizations to residents in real time, delivering information to geographically targeted con sumers over their cell phones (via text messages), through e-mails and via Web access. Nixle has a partnership with NLETS (the International Justice and Public Safety Network), a secure information sharing system for state and local law enforcement agencies. Nixle is free to all governments and consumers.

http://www.nixle.com/

http://www.nixle.com/citizen_faqs.html

http://local.nixle.com/city/md/baltimore/

http://local.nixle.com/city/pa/harrisburg/

http://local.nixle.com/city/ky/fort-knox/

Facebook®. Facebook is a social networking Web site. Users can add friends and send them messages, and update their personal profiles to notify friends about them selves. Users can join networks organized by city, work place, school and region.

http://www.facebook.com/help/new_user_guide.php

http://ro-ro.facebook.com/ChicagoPoliceDepartment

http://sk-sk.facebook.com/pages/Los-Angeles-CA/UCLA-Police-Department/54881942710?ref=mf

http://www.facebook.com/pages/Duluth-MN/Duluth-Minnesota-Police-Department/93899422988

How to Set Up a Facebook Account

http://www.ehow.com/how_2081063_set-up-facebook-account.html

How to Set Up a Facebook Profile

http://www.ehow.com/how_4464690_set-up-facebook-profile.html

MySpace™. MySpace is a social networking Web site with an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos and music

http://faq.myspace.com/app/home

http://www.myspace.com/limestonepd

http://www.myspace.com/fayettevillepolice

http://www.myspace.com/fairfieldpolice

How to Set Up a MySpace Page

http://www.ehow.com/how_5225868_set-up-myspace-step-step.html

How to Set Up Your MySpace Profile

http://www.dummies.com/how-to/content/how-to-set-up-your-myspace-profile.html

YouTube™. YouTube is a video sharing Web site on which users can upload and share videos.

http://www.youtube.com/

Flickr®. Flickr is an image and video hosting Web site, Web services suite and online community platform. In addi tion to being a popular Web site for users to share personal photographs, the service is used by bloggers as a photo repository.

http://www.flickr.com/about/

http://www.flickr.com/photos/bcorreira/3752736180/

http://www.flickr.com/photos/44683348@N00/

FriendFeed. FriendFeed pulls together other social media sites into one destination. It is a real-time feed aggre gator that consolidates the updates from social media and social networking Web sites, social bookmarking Web sites, blogs and micro-blogging updates. It is possible to use this stream of information to create customized feeds to share, as well as originate new posts discussions (and comment) with friends. Users can be an individual, business or organization.

http://friendfeed.com/about/help