washingtonpost.com

National Dragnet Is a Click Away

Authorities to Gain Fast and Expansive Access to Records

By Robert O'Harrow Jr. and Ellen Nakashima
Washington Post Staff Writers
Thursday, March 6, 2008; A01

Several thousand law enforcement agencies are creating the foundation of a domestic intelligence system through computer networks that analyze vast amounts of police information to fight crime and root out terror plots.

As federal authorities struggled to meet information-sharing mandates after the Sept. 11, 2001, terrorist attacks, police agencies from Alaska and California to the Washington region poured millions of criminal and investigative records into shared digital repositories called data warehouses, giving investigators and analysts new power to discern links among people, patterns of behavior and other hidden clues.

Those network efforts will begin expanding further this month, as some local and state agencies connect to a fledgling Justice Department system called the National Data Exchange, or N-DEx. Federal authorities hope N-DEx will become what one called a "one-stop shop" enabling federal law enforcement, counterterrorism and intelligence analysts to automatically examine the enormous caches of local and state records for the first time.

Although Americans have become accustomed to seeing dazzling examples of fictional crime-busting gear on television and in movies, law enforcement's search for clues has in reality involved a mundane mix of disjointed computers, legwork and luck.

These new systems are transforming that process. "It's going from the horse-and-buggy days to the space age, that's what it's like," said Sgt. Chuck Violette of the Tucson police department, one of almost 1,600 law enforcement agencies that uses a commercial data-mining system called Coplink.

With Coplink, police investigators can pinpoint suspects by searching on scraps of information such as nicknames, height, weight, color of hair and the placement of a tattoo. They can find hidden relationships among suspects and instantly map links among people, places and events. Searches that might have taken weeks or months -- or which might not have been attempted, because of the amount of paper and analysis involved -- are now done in seconds.

On one recent day, Tucson detective Cynthia Butierez demonstrated that power in an office littered with paper and boxes of equipment. Using a regular desktop computer and Web browser, she logged onto Coplink to search for clues about a fraud suspect. She entered a name the suspect used on a bogus check. A second later, a list of real names came up, along

with five incident reports.

She told the system to also search data warehouses built by Coplink in San Diego and Orange County, Calif. -- which have agreements to share with Tucson -- and came up with the name of a particular suspect, his age and a possible address. She asked the software to find the suspect's links to other people and incidents, and then to create a visual chart displaying the findings. Up popped a display with the suspect at the center and cartoon-like images of houses, buildings and people arrayed around him. A final click on one of the houses brought up the address of an apartment and several new names, leads she could follow.

"The power behind what we have discovered, what we can do with Coplink, is immense," Tucson police Chief Richard Miranda said. "The kinds of things you saw in the movies then, we're actually doing now."

Intelligence-Led Policing

The expanding police systems illustrate the prominent roles that private companies play in homeland security and counterterrorism efforts. They also underscore how the use of new data -- and data surveillance -- technology to fight crime and terrorism is evolving faster than the public's understanding or the laws intended to check government power and protect civil liberties, authorities said.

Three decades ago, Congress imposed limits on domestic intelligence activity after revelations that the FBI, Army, local police and others had misused their authority for years to build troves of personal dossiers and monitor political activists and other law-abiding Americans.

Since those reforms, police and federal authorities have observed a wall between law enforcement information-gathering, relating to crimes and prosecutions, and more open-ended intelligence that relates to national security and counterterrorism. That wall is fast eroding following the passage of laws expanding surveillance authorities, the push for information-sharing networks, and the expectation that local and state police will play larger roles as national security sentinels.

Law enforcement and federal security authorities said these developments, along with a new willingness by police to share information, hold out the promise of fulfilling post-Sept. 11, 2001, mandates to connect the dots and root out signs of threats before attacks can occur.

"A guy that's got a flat tire outside a nuclear facility in one location means nothing," said Thomas E. Bush III, the FBI's assistant director of the criminal justice information services division. "Run the guy and he's had a flat tire outside of five nuclear facilities and you have a clue."

In a paper called "Intelligence-Led Policing: The New Intelligence Architecture," law enforcement authorities working with the Justice Department said officers " 'on the beat' are an excellent resource for gathering information on all kinds of potential threats and vulnerabilities."

"Despite the many definitions of 'intelligence' that have been promulgated over the years, the simplest and clearest of these is 'information plus analysis equals intelligence,' " the paper said.

Efforts by federal authorities to create national networks have had mixed success.

The federal government has long successfully operated programs such as the Regional Information Sharing System, which enables law enforcement agencies to communicate, and the National Crime Information Center, an index of criminal justice information that police across the country can access. Though successful, those systems offer a relatively limited look at existing records.

A Department of Homeland Security project to expand sharing substantially, called the Information Network, has been bedeviled by cost overruns, poor planning and ambivalence on the part of local and state authorities, according to the Government Accountability Office. Almost every state has established organizations known as intelligence fusion centers to collect, analyze and share information about possible leads. But many of those centers are underfunded and undermanned, and some of the analysts are not properly trained, the GAO said last year.

Federal authorities have high hopes for the N-DEx system, which is to begin phasing in as early as this month. They envision a time when N-DEx, developed by Raytheon for $85 million, will enable 200,000 state and local investigators, as well as federal counterterrorism investigators, to search across millions of police reports, in some 15,000 state and local agencies, with a few clicks of a computer mouse. Those reports will include names of suspects, associates, victims, persons of interest, witnesses and any other person named in an incident, arrest, booking, parole or probation report.

The system will be accessible to federal law-enforcement agencies, such as the FBI, and state fusion centers. Intelligence analysts at the National Counterterrorism Center and FBI's Foreign Terrorist Tracking Center likely will have access to the system as well.

"The goal is to create a one-stop shop for criminal justice information," the FBI's Bush said.

In the meantime, local and state authorities have charged ahead with their own networks, sometimes called "nodes," and begun stitching them together through legal agreements and electronic links.

At least 1,550 jurisdictions across the country use Coplink systems, through some three dozen nodes. That's a huge increase from 2002, when Coplink was first available commercially.

At least 400 other agencies are sharing information and doing link analysis through the Law Enforcement Information Exchange, or Linx, a Navy Criminal Investigative Service project built by Northrop Grumman using commercial technology. Linx users include more than 100 police forces in the District, Virginia and Maryland.

Hundreds of other police agencies across the country are using different information-sharing systems with varying capabilities. Officials in Ohio have created a data warehouse containing the police records of nearly 800 jurisdictions, while leaving it to local departments to provide analytical tools.

Same Data, New Results

Authorities are aware that all of this is unsettling to people worried about privacy and civil liberties. Mark D. Rasch, a former federal prosecutor who is now a security consultant for FTI Consulting, said that the mining of police information by intelligence agencies could lead to improper targeting of U.S. citizens even when they've done nothing wrong.

Some officials avoid using the term intelligence because of those sensitivities. Others are open about their aim to use information and technology in new ways.

One widely used Coplink product is called Intel Lead. It enables agencies to enter new information, tips or observations into the data warehouses, which can then be accessed by people with proper authority. Another service under development, called "predictor," would use data and software to make educated guesses about what could happen.

"Intel Lead is particularly applicable to the needs of statewide criminal intelligence and antiterrorism fusion centers as well as federal agencies who need to bridge the intelligence gap," said a news release by Knowledge Computing, the company that makes Coplink.

Robert Griffin, the chief executive of Knowledge Computing, said Coplink yields clues and patterns they otherwise would not see. "It's de facto intelligence that's actionable," Griffin said.

Managers of Linx are eager to distinguish their system from the commercial Coplink and its more extensive capabilities. They acknowledge their system includes data-analysis capabilities, and it will feed information to counterterrorism and intelligence authorities. In fact, the system is designed to serve as a bridge between law enforcement and intelligence.

But they said Linx is not an intelligence system under federal laws, because it relies on records police have always kept. "It does not create intelligence," said Michael Dorsey, the Naval Criminal Investigative Service special agent in charge. "It creates knowledge."

To allay the public's fears, many police agencies segregate information collected in the process of enforcing the law from intelligence gathered on gangs, drug dealers and the like. Projects receiving federal funding must do so.

Nearly every state and local jurisdiction has its own guides for these new systems, rules that include restrictions intended to protect against police intrusiveness, authorities said. The systems also automatically keep track of how police use them.

N-DEx, too, will have restrictions aimed at preventing the abuse of the data it gathers. FBI officials said that agencies seeking access to N-DEx would be vetted, and that only authorized individuals would have access. Audit trails on whoever touches a piece of data would be kept. And no investigator would be allowed to take action -- make an arrest, for instance -- based on another agency's data without first checking with that agency.

But even some advocates of information-sharing technology worry that without proper oversight and enforceable restrictions the new networks pose a threat to basic American values by giving police too much power over information. Timothy Sample, a former intelligence official who runs the Intelligence and National Security Alliance, is among those who think computerized information-sharing is critical to national security but fraught with risks.

"As a nation, our laws have not kept up," said Sample, whose group serves as a professional association of intelligence officials in the government and intelligence contracting executives in the private sector.

Thomas McNamara, chief of the federal Information Sharing Environment office, said a top goal of federal officials is persuading regional systems to adopt most of the federal rules, both for privacy and to build a sense of confidence among law enforcement authorities who

might be reluctant to share widely because of security concerns.

"Part of the challenge is to leverage these cutting-edge tools so we can securely and appropriately share that information which supports efforts to protect our communities from future terrorist attacks," McNamara said. "Equally important is that we do so in a manner that fully protects the information privacy and legal rights of all Americans."

Miranda, the Tucson police chief, said there's no overstating the utility of Coplink for his force. But he too acknowledges that such power raises new questions about how to keep it in check and ensure that the trust people place in law enforcement is not misplaced.

"I don't want the people in my community to feel we're behind every little tree and surveilling them," he said. "If there's any kind of inkling that we're misusing our power and our technology, that trust will be destroyed."