

Monday, August 29, 2005



Long arm of the law

Enterprising law enforcement agencies use new technologies to spur cross-border data sharing

By Alan Joch

Published on Aug. 29, 2005

Homeland security officials have long known that their success depends on acting locally but thinking globally. Now, as they work to keep terrorists from crossing international borders, some law enforcement organizations are focusing global efforts on making it easier for information about crimes and criminals to flow from one country to the next.

"Terrorism is a global problem, and law enforcement agencies have to get rid of the boundaries between domestic anti-terrorism and international anti-terrorism efforts — they're the same thing," said Paul Wormeli, executive director of the Integrated Justice Information Systems Institute, a nonprofit corporation formed by information technology companies to advocate for better data sharing among public organizations.

International collaboration for homeland security is happening to some degree, partially thanks to Extensible Markup Language standards tailored specifically for law enforcement. But turf battles, legal and political roadblocks, and privacy fears all stand in the way of wider information collaboration across borders.

"Think about the conundrum of sharing law enforcement data," said Jeff Pollock, chief technology officer at Cerebra, a vendor of data-sharing technology with offices in the United Kingdom and United States.

"On the one hand, authorities need central access to up-to-date information, while on the other hand, civil

ADVERTISEMENT

I Rely on GTSI

The HP Deskjet 450wbt Wireless Mobile Printer

BUY NOW! ▶

I Rely on GTSI

HP nw8240 Mobile Workstation

BUY NOW! ▶

liberties groups are adamant about not creating central databases that make it easier for hackers to gain access to a lot of personal information," Pollock said. "Also, data is collected by a number of different sources, including federal, state and local. Agencies are reluctant to let go of the ownership of their data."

Despite the hurdles, examples of international data sharing offer hope for law enforcement officials anxious for more watch lists and other tools and information that countries could exchange.

Continental view

Data collaboration has some well-established roots in Europe. Interpol, the international police organization headquartered in Lyon, France, manages a stolen travel documents database that holds more than 5 million records, which are available to countries throughout Europe. European countries carried out more than 2,700 searches in the first quarter of this year, said Ronald Noble, Interpol's secretary general.

Interpol's I-24/7 system also distributes online records of fingerprints, DNA profiles and photos of wanted criminals from more than 17 countries. The system uses a virtual private network to provide secure e-mail and the ability to query Interpol's database of international arrest warrants, known as Red Notices. Interpol is sponsoring a pilot program with the FBI to use I-24/7 to share the bureau's stolen motor vehicle database with 60 countries.

Similarly, Europol, the European Union's criminal intelligence agency, is developing an electronic system to share data among EU states.

Law enforcement agencies throughout England, Wales and eventually Scotland are sharing information through the National Automated Fingerprint Identification System, which connects the computers and fingerprint scanning systems of nearly 50 police forces and agencies. It can compare more than 8 million fingerprints per second.

The system is limited to the United Kingdom, but managers at the Police Information Technology Organisation (PITO) in London say it has global implications.



RELATED LINKS

[A new spin on global security](#)

[Israel uses hands-on approach for trusted travelers](#)

[Hong Kong airport tunes](#)

Data that speaks for itself

Many law enforcement and government experts view the development of Semantic Web technology as a catalyst for better information sharing and analysis. The technology is based on evolving standards from the World Wide Web Consortium, one of the main Web standards bodies. They provide sophisticated descriptors of Web content.

Extensible Markup Language relies on two main components: the document and the schema, which defines the document's structure. Semantic Web technology builds on this foundation by adding more information about the relationships among various schema components. The result: "Software can understand what data means in relation to other pieces of data," said Jeff Pollock, chief technology officer at Cerebra, a vendor of data-sharing technology with offices in the United Kingdom and United States.

"Many groups are looking at how [biometric] data can be shared and used internationally," said Colin Patton, deputy director for identification at PITO, which supplies IT services and equipment to police departments throughout the United Kingdom.

Patton said the fingerprint system could act as a building block for other projects.

"As we look across the [United Kingdom] and internationally, systems like these must be capable of sharing data with other programs," he said.

Crime-fighting XML

One of the two keys to the U.K. system's data-sharing capabilities is the corporate data model PITO created for police services. The model standardizes the formatting of names, birth dates and other data elements.

"It's fine to talk about new technologies, but even more critical for sharing information are the actual data structures and the ability to have a common understanding of what the data represents," Patton said.

The second key is XML. "It's what gives everyone access to the data," said Rod Forry, program manager at Northrop Grumman IT, the systems integrator that helped launch the system. A frame-relay backbone — soon to be replaced by Multiprotocol Label Switching (MPLS) networking — provides the pipeline for distributing data to police departments, Forry said.

Although XML was first adopted by commercial businesses in the 1990s, law enforcement IT managers worldwide soon embraced it as a tool for smoothing processes such as the distribution of police arrest reports to prosecutors or officers in other jurisdictions. But for years, "it was missing a vocabulary for law enforcement," Wormeli said.

That missing link came with Global Justice XML (GJXML), an XML adaptation created by the U.S. Justice Department's Office of Justice Programs and the Global Justice Information Sharing Initiative, a consortium of 32 local, state, federal and international justice organizations.

GJXML provides a data model, a data dictionary and schemas tailored to law enforcement. Those tools free agencies from writing custom interfaces for data sharing. "It's being adopted by law enforcement at breakneck speed," Wormeli said.

The next step for greater data interoperability will be Semantic Web technology, many law enforcement IT experts say.

"Semantic technology hasn't really hit the justice world yet, but it could do so in the next year or so," Wormeli said. "It's an evolutionary step forward for aggregating information from multiple databases

Eventually, Semantic Web technology might help agencies more effectively cross the chasm between structured data held in relational databases and free-form information in word-processing documents, such as witness statements.

"There is a lot of intelligence held in free-form text, and with semantics, we can extract that information and link it with other entities," said Tom Golding, business development director at Semagix, a semantic technology vendor with offices in London and White Plains, N.Y.

The company's technology, which the London police are evaluating, can look for data relationships across internal and external databases and text documents to uncover background information about a terrorism suspect.

— Alan Joch

for actionable intelligence."

Dave Mitchelhill, chief technology officer of Criminal Justice IT in London, an agency that works to link police, court and related networks, said he believes semantic technology will eventually become a significant tool for data collaboration. "We're seriously looking at the technology, but we're moving in baby steps," he said.

Semantic technology could help organizations that share data across borders deal with another country's IT authorities, who could impose data formatting rules and data dictionaries.

"Thus, in the [United Kingdom,] we may use the term 'magistrate' to refer to a junior court judge," Mitchelhill said. "But if we join up with law enforcement systems elsewhere on the continent, a 'magistrate' may refer to an investigator. We can't expect the French to change their terminology, and we're not going to change ours. That's why we need semantic technology to understand the context of the data and move it across the systems."

Culture wars

Although GJXML and semantic technology provide easier ways for organizations to share data, technology isn't the only factor. Many observers say cultural, legal and political considerations play a much bigger role in determining the quantity of international information sharing.

Although it's not yet an international effort, a project in the Pacific Northwest, which may eventually include Canadian authorities, shows the promise and concerns of interagency data sharing.

The Law Enforcement Information Exchange (Linx) brings together federal, state and local law enforcement agencies using a data warehouse and analysis applications that can mine information from the data store. The FBI launched the project after the Sept. 11, 2001, terrorist attacks, but the bureau withdrew its support after two years.

Believing the area still needed the system, local leaders picked up the effort using financing from the Naval Criminal Investigative Service (NCIS), a law enforcement and counterintelligence arm of the Navy. Linx now holds a variety of data, including investigation records, witness statements and arrest reports, which are available to NCIS; the Washington State Patrol; local, county and city police; and Port of Seattle authorities.

"If an officer stops someone and only has license plate information, the system can go out to disparate federal and local data sources and return the results right to the squad car," said Tony Crescenzo, vice president and public-sector general manager at Initiate Systems. The company contributed data-integration tools that combine records from different databases.

Earlier this year, the system's ability to cross-check information from various sources paid off. A detective in Kitsap County, Wash., arrested a person suspected of passing bad checks. While running a background check using Linx, the detective discovered connections between the suspect and other cases in a county in the eastern part of Puget Sound.

After obtaining search warrants, law enforcement officers arrested a handful of people involved in check fraud activities by linking their activities via the data warehouse.

The arrests aren't likely to turn the tide in international anti-terrorism efforts, but this example is symbolic, said Dan Estrem, a former counterterrorism agent who spent 20 years with the FBI and is now a consultant at the Center for Strategic Management. Estrem is the lead project manager for Linx.

"This was one of the first cases where detectives used the system to link incident records and free-form text documentation from investigative records, and it led to significant arrests," Estrem said. "One of the people arrested told detectives he thought they would be a bunch of backwoods hicks who couldn't follow up on the crimes, so he thought he was safe."

This success helps break down the cultural stumbling blocks that inhibit data sharing, Estrem said. "The primary hurdle is lack of trust," he said. "It's endemic everywhere from the five-man police department in rural America to international agencies. Information is power, and if I know something, I can act on it. If you know what I know, you can act on it. So there are always concerns of case jumping and stealing sources."

In addition, some laws seek separation of power that precludes data sharing among local authorities with federal or international organizations.

"Individual agencies don't have to share data, and the feds can't order them to do it," Estrem said. "Instead, the groups have to decide to partner" voluntarily in anti-terrorism and other crime-fighting efforts.

To promote the interchange within Linx, participating members drafted formal rules of operation that spell out how individual entities retain control of the data they collect. Police chiefs, sheriffs and other officials also meet regularly to discuss new procedural and security questions.

Four other regions are using or introducing Linx networks, including 14 agencies, soon to grow to 28, near Hampton Roads, Va.; about 30 agencies near Kings Bay, Ga.; 30 agencies near Corpus Christi, Texas; and others in Honolulu.

Estrem said the Royal Canadian Mounted Police wants to test data sharing with Seattle's Linx users, but they must resolve several cross-border issues.

"It's national politics, not agency-to-agency interactions, that are holding things back," Estrem said. "We need State Department authority and treaties to be signed to make this happen." n

Joch is a business and technology writer based in New England. He can be reached at ajoch@monad.net.

Worth the effort

International data sharing offers many benefits, such as:

- Identifying terrorists through combined watch lists.
- Locating identity theft and money laundering rings that fund terrorist activities.
- Linking database records and witness statements to build cases.

But hurdles remain, including:

- A lack of technology for combining database records. Free-form text is still maturing.
- Agency bias against sharing data with other organizations.
- Regulations that restrict the flow of personal and criminal information across borders.

— Alan Joch