



Los Angeles County, California



Introduction and Purpose

The ability of law enforcement agencies to combat crime and terrorism depends on their ability to acquire, assess, analyze, and share information. Information sharing improves operations in many ways—

- It increases **situational awareness** for officers on the street by providing information about people, places, vehicles, and situations they encounter while on patrol.
- It affords detectives and investigators the ability to understand more thoroughly the **circumstances of an incident or subject** under investigation.
- It allows law enforcement executives to understand **crime trends and other factors** relevant to effective strategies for information-led, community-oriented policing.
- It supports the **National Strategy for Information Sharing**, which relies on state, local, and tribal law enforcement agencies to collect, analyze, and share information about suspicious persons and activities with their counterparts in neighboring jurisdictions, as well as with Federal partners.

In a large metropolitan area, such as Los Angeles County, California, information sharing between jurisdictions becomes even more important. It is often said that criminals do not respect jurisdictional boundaries, and that crime trends are a regional problem whose solution demands a cross-jurisdictional, collaborative solution. Information sharing is at the core of this solution.

While this case study necessarily discusses the specific technologies used in Los Angeles County, this does not imply SEARCH's endorsement or recommendation of these products. There are several products in the marketplace with which law enforcement agencies can build similar systems.

The focus of this case study is on the partnership, governance, business goals, features, and overall technical approach of the solution. These factors will have relevance to most systems, regardless of the specific technologies chosen.

This *Information Sharing Case Study* was developed by SEARCH, The National Consortium for Justice Information and Statistics, under Cooperative Agreement 2007-DD-BX-K102 awarded by the U.S. Department of Justice Office of Justice Programs Bureau of Justice Assistance. Scott Came, Director of Systems and Technology, SEARCH, was the primary author of this case study. Points of view or opinions contained in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Francis X. Aumand III
Chairman

Ronald P. Hawley
Executive Director

Kelly J. Peters
Deputy Executive Director

SEARCH
7311 Greenhaven Drive, Suite 145
Sacramento, CA 95831
(916) 392-2550 • (916) 392-8440 (fax)
www.search.org

This document contains a case study of law enforcement information sharing in Los Angeles County, California. It is the result of interviews and analysis that SEARCH, The National Consortium for Justice Information and Statistics, conducted in March 2009 with staff from the Los Angeles County Sheriff's Department. The goal of the case study is to provide other law enforcement agencies and consortia with the background on this successful information sharing effort, with the hope that the techniques, technologies, and lessons learned in Los Angeles County will assist and accelerate similar efforts elsewhere.

Solution Overview

The details of Los Angeles County's information sharing system will appear later in this case study; however, it is important to describe the system at a high level at the outset so the entire document is placed in proper context.

In 2006, the Los Angeles County Sheriff's Department (LASD) implemented a centralized database for the department that contained records management system (RMS), computer-aided dispatch (CAD), traffic citation, and jail booking information. This database, called a *data warehouse*, tied the information from these disparate systems together into a cohesive, common format that LASD personnel could query easily, rather than having to use separate tools and techniques to query the four underlying systems separately.

The data warehouse, named the **Incident Reporting Information System (IRIS)**, includes a sophisticated query interface (computer program) that allows users across the department to search the four data sources by personal identifiers (name, date of birth, drivers license number, etc.), vehicle (make, model, color, license plate number, etc.), locations, and more. The solution leverages COPLINK® software from Knowledge Computing Corporation (KCC).

While LASD was building its data warehouse, the Los Angeles Police Department (LAPD) was deploying a similar solution with the same technology. Other jurisdictions in southern California, including several cities in neighboring Orange County and nearby San Diego and Imperial Counties, were either implementing or investigating the solution as well. Ultimately, common interests and a recognition that crime in southern California is a regional issue led LASD, LAPD, and the Los Angeles County Police Chiefs' Association to establish the **Regional Terrorism Integrated Information System (RTIIS)**. The system has grown to include information from 45 independent municipal police agencies in the county, and is expanding to include school district, port authority, and campus police forces as well. The RTIIS system includes RMS data from each participating municipal police agency and leverages common technology—COPLINK—to tie the individual cities' information with the LAPD and LASD data warehouses (Figure 1).

The Business Problem

It is a well-known best practice of technology strategy to implement solutions only after gaining a clear understanding of the business problem that the technology will address.¹ LASD developed a vision of departmentwide information sharing in 2006, and that vision provided the foundation for both IRIS and RTIIS.

Captain Scott Edson of LASD reports that both departmental and countywide information sharing have become a cornerstone of LASD's strategy. "The focus is on what we call the *Four A's*: Acquire, Assess, Act, and Accountability," said Edson. "We have created a culture of acquiring information from our daily operations, because everyone understands how important complete and accurate information is. We have invested in the assessment of information, through a centralized crime analysis program and the deployment of IRIS. We practice information-led policing, meaning that we drive our actions from information that is available to every officer, regardless of rank, at all times. And information supports accountability, from the public through the Sheriff through the command staff to the officers on the street—we set goals and measure our progress. Then the cycle starts over again with acquisition."

Within this overall strategy framework, IRIS and RTIIS address five key business needs for LASD and the other RTIIS partners.

¹ This best practice is described in many publications, including these developed by SEARCH: *Information Systems Integration: A Library of SEARCH Resources for Justice and Public Safety Practitioners* (Sacramento, CA: SEARCH, 2004). Available at <http://www.search.org/files/pdf/IntegrationLibrary.pdf>. *Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!)*, *A Guide for Executives, Managers and Technologists*, Kelly J. Harris and William H. Romesburg (Washington, D.C.: U.S. Department of Justice Office of Community Policing Services, 2002) at Chapter 4. Available at <http://www.search.org/files/pdf/TECHGUIDE.pdf>.

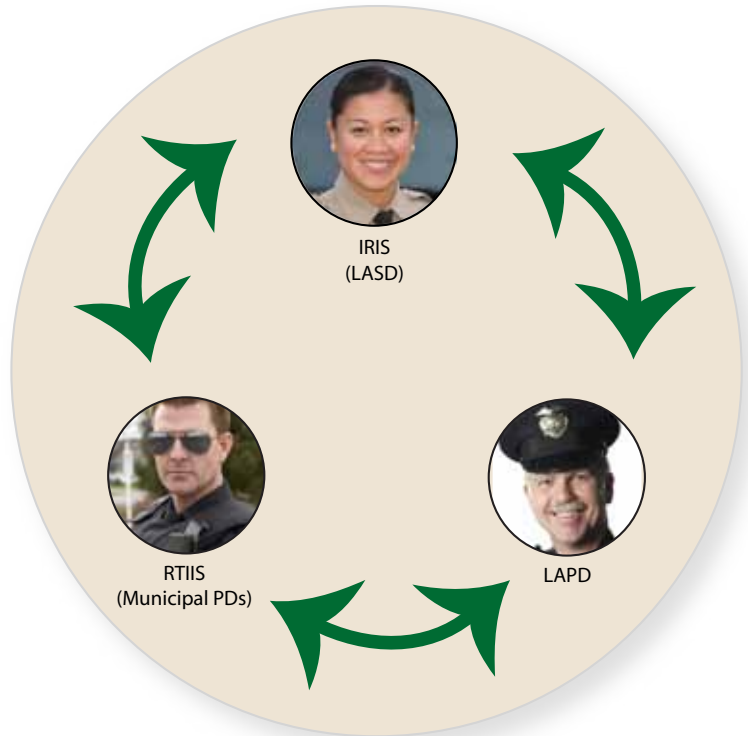


Figure 1: Officers from Different Agencies in Los Angeles County Get the Same Information Via Three COPLINK Nodes

► Improved Situational Awareness

Peace officers are safer and more effective when they know more about their surroundings and the situations in which they work. An officer's approach to a subject will be more cautious if she knows the subject has a history of violence toward law enforcement, or if he has had recent encounters of a similar nature in neighboring jurisdictions. An officer might also conduct a more effective field interview if he has full knowledge of recent interviews with officers on the other side of the county.

Captain Edson from the LASD also leverages the power of shared information for what he calls *intentional patrol*. "Some time ago, officers maintained considerable situational awareness just by listening to the radio," he explained. "A deputy would pick up on patterns of burglaries, or vandalism, or drug crimes in particular areas from radio traffic. However, our department has shifted non-priority communications to text on a mobile data terminal (MDT). As a result, if it's not priority traffic, deputies often don't hear about it. An information sharing system gives us a way to inform officers about what's going on in the areas they patrol, allowing them to focus their time strategically—and intentionally. That's intentional patrol, and we accomplish it without congesting radio channels."

IRIS Provides Key Details that Help Apprehend Bike Thief

In February 2009, a male suspect committed grand theft at a sporting goods store in La Cañada Flintridge by stealing a bicycle valued at \$699. Less than two weeks later, the same suspect entered the same store and again went directly to the bicycle section and began asking employees questions. The loss prevention person on duty recognized the individual as the same person who had previously stolen a bicycle.

The witness obtained the license plate number and description of the suspect's vehicle. An LASD Crime Analyst ran the license number in the department's Justice Data Interface Controller (JDIC) to determine the registered owner's name and address. The analyst then used IRIS and Lexis to identify persons in addition to the owner who might have access to the vehicle.

A 26-year-old man was identified as a possible suspect based on his physical descriptors, the fact that he lived at the address with the vehicle's owner, past incidents, and participants associated with the owner's address, according to IRIS. The investigating detective was provided with information about the possible suspect. Witnesses then positively identified the suspect and still photos from surveillance footage confirmed that it was the same individual.

A search warrant was executed in March 2009, and the suspect arrested and held on no bail for several parole violations. His probation officer stated, "He is going to prison this time. This was his last chance." The stolen property from the theft in February was also recovered.

► Improved Investigative Capabilities

Criminal investigations are more effective if patrol officers have adequate information to begin the investigation while responding to incidents and when contacting subjects for the first time. Armed with current data about people, places, vehicles, and locations, front-line officers can handle some investigative responsibilities at the scene that in the past required consultation with a detective over a period of hours or days. As a result, incident reports and field interviews become a richer, more complete source of information for detectives and prosecutors to use as they build their cases. In some situations, increased on-scene investigative capabilities leads to the capture of information and evidence that would otherwise be overlooked and lost.

Engaging more personnel in the capture of information and the conduct of investigations improves overall law enforcement efficiency. Detectives can more effectively plan and prioritize their work, and can spend more time on analysis and case-building because front-line officers have captured more of the raw information they need.

► Addressing Crime as a Cross-Jurisdictional Issue

The Law Enforcement Information Sharing Program (LEISP) at LASD has this motto: "Know Crime, No Boundaries." Like many sheriff's departments, LASD covers a patchwork of territories that includes portions of unincorporated county jurisdiction between cities, as well as contract work for municipal jurisdictions. Yet the criminals (and potential terrorists) that the department encounters have little concern for or even awareness of these boundaries. As perpetrators detect one jurisdiction's effort to attack a particular crime problem, they can simply shift their operations to a nearby area, but to the citizens and businesses in the community overall, the problem still exists.

Information sharing within a region certainly helps agencies collaborate across political and geographical boundaries. Technology can present a seamless view of people, places, and things to officers across a region. But in addition to the information itself, creating a culture of sharing is an important element of taking a cross-jurisdictional, collaborative approach to fighting crime. It encourages the leaders of law enforcement agencies to recognize areas of common purpose and to formalize how they work with one another.

► Better Leveraging of Information in Operational Systems

Like many jurisdictions, the LASD and its partners have invested substantial resources in operational systems. The RMS and CAD system used by the LASD contain 5.5 million and 43 million records, respectively. These data sources contain information critical to the Department's ability to interact effectively with subjects, respond appropriately to incidents, and to investigate and solve crimes. However, it is generally much easier to put information *into* operational systems than it is to get the data *out of* these systems in an easy-to-use, meaningful way. The challenge grows exponentially with each new data source, as information users have to deal with separate systems and separate data formats, especially across jurisdictional boundaries. The wealth of information is obscured or locked away behind technology and usability barriers.

Properly designed and implemented information sharing systems like IRIS and RTIIS can unlock the rich information assets in law enforcement agencies by presenting information consumers with common tools and an interface designed primarily to get information out rather than putting it in. In the end, enabling a cohesive, integrated view of an agency's information significantly increases the return on the initial investment in the source systems.

Burglary Suspect Nabbed Via COPLINK Use

In February 2008, a Crime Analyst with the LASD's Crescenta Valley Station was able to use COPLINK to locate the registered owner of a vehicle parked near a residential burglary after a witness reported the vehicle license number.

The registered owner was not at the address of record and the owner's mother stated she had no idea where her daughter lived or worked.

Using COPLINK, the analyst was able to find a work telephone number for the registered owner based on the owner being listed as an Emergency Contact for an arrestee. Once contacted at her place of employment, the vehicle's owner stated that her ex-boyfriend was the driver of the vehicle and that she had no idea where to locate him.


Using COPLINK again, the analyst was able to assist detectives in identifying the suspect, his associates, and known hangouts in Pasadena. The suspect information was passed to detectives in Altadena and Pasadena.

The suspect's vehicle was seen in Altadena near the scene of residential burglaries, and the suspect was arrested by the Pasadena Police Department for a residential burglary in their city.



“Combining advanced technology and information sharing techniques with dedicated policing gets results.”

**—Leroy D. Baca, Sheriff
Los Angeles County Sheriff's Department**



► **Increased Participation in the National Law Enforcement Community**
The National Strategy for Information Sharing identifies a critical role for state, local, and tribal law enforcement organizations in the nation’s approach to combating terrorism.²

Information Sharing with State, Local, and Tribal Entities. As our Nation’s first “preventers and responders,” State, local, and tribal governments are critical to our efforts to prevent future terrorist attacks and to respond if an attack occurs. They must have access to the information that enables them to protect our local communities. In addition, these State, local, and tribal officials are often best able to identify potential threats that exist within their jurisdictions. They are full and trusted partners with the Federal Government in our Nation’s efforts to combat terrorism, and therefore they must be a part of an information sharing framework that supports an effective and efficient two-way flow of information enabling officials at all levels of government to counter and respond to threats.

— From *National Strategy for Information Sharing*, at page 3

This same philosophy applies to a nationally coordinated effort to fight crime as well.

Implementing this strategy requires (a) that information flow from the source systems—the police RMS, field reporting, and CAD systems—to national repositories like the Federal Bureau of Investigation’s Law Enforcement National Data Exchange system (FBI N-DEx),³ and (b) that local law enforcement agencies can, in turn, query these national repositories to enhance the information they collect locally. In addition, local information should flow to the state and urban area fusion centers, facilitated by standards such as the Suspicious Activity Reporting (SAR) functional standard⁴ published by the Program Manager for the Information Sharing Environment (PM-ISE).

Enabling the flow of information from state, local, and tribal law enforcement agencies to Federal partners and fusion centers will only happen if technology can connect the underlying systems and transform the data in a way that minimizes the cost burden on the contributing agencies. Small agencies in particular simply do not have the resources to share information locally and nationally; even large agencies will find participation in national efforts like N-DEx and the Nationwide SAR Initiative (NSI)⁵ more compelling if local information sharing systems can act as a “bridge” between their systems and national systems. Integrated local systems offer a chance to spread the costs of participating in national initiatives across a larger group of partners, and simultaneously improve the consistency and timeliness of reporting.

2 *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, D.C.: National Security Council, October 2007). Available at http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf.

3 See the FBI N-DEx page at http://www.fbi.gov/hq/cjis/ndex/ndex_home.htm.

4 See the SAR functional standard page at <http://niem.gtri.gatech.edu/niemtools/iepd/display/container.iepd?ref=ntsXeIX7M6Q%3D>.

5 See the National Criminal Intelligence Resource Center’s NSI page at <http://www.ncirc.gov/sar>.

The Partners

The Los Angeles County Sheriff’s Department (LASD) is the largest sheriff’s department in the world with a law enforcement jurisdiction of 3,157 square miles of the county’s 4,084 square miles and serving a population of approximately 4 million of the county’s more than 10 million residents. Additionally, LASD provides law enforcement services to 9 community colleges, the Metropolitan Transportation Authority, 48 Superior Courts, and residents living in the County’s 90 unincorporated communities and 40 contract cities. The department is also responsible for managing and securing approximately 19,000 inmates in eight custody facilities.

LASD provides patrol services through 23 stations spread out through Los Angeles County. The patrol environment consists of dense urban areas, desert, national forest, rural communities, beaches, harbors, and Catalina Island. LASD is budgeted for 10,000 sworn personnel and another 8,000 civilian personnel. It handles in excess of 1 million calls a year, and handled 85,784 Part I crimes in calendar 2008.

LASD is working on behalf of the Los Angeles County Police Chiefs’ Association in implementing RTIIS.

- Alhambra
- Arcadia
- Azusa
- Baldwin Park
- Bell
- Bell Gardens
- Beverly Hills
- Burbank
- Claremont
- Covina
- Culver City
- Downey
- El Monte
- El Segundo
- Gardena
- Glendale
- Glendora
- Hawthorne
- Hermosa Beach
- Huntington Park
- Inglewood
- Irwindale
- La Verne
- Long Beach
- Manhattan Beach
- Maywood
- Monrovia
- Montebello
- Monterey Park
- Palos Verdes
- Pasadena
- Pomona
- Redondo Beach
- San Fernando
- San Gabriel
- San Marino
- Santa Monica
- Sierra Madre
- Signal Hill
- South Gate
- South Pasadena
- Torrance
- Vernon
- West Covina
- Whittier



This map shows the vastness of Los Angeles County, as well as the broad-based participation in RTIIS by 45 municipal police agencies.

A consortium of 47 partner agencies collaboratively governs RTIIS. The partners include LASD, the Los Angeles Police Department, and 45 municipal police agencies in the county. As a result, RTIIS is a comprehensive repository of countywide law enforcement information.

The RTIIS governance structure consists of a five-agency governance committee that makes decisions on behalf of the 45 municipal partners. Currently the five committee members are LAPD, LASD, and the police departments of Hawthorne, Monrovia, and Long Beach. The governance committee is empowered to establish ad-hoc working groups as needed, although in practice ad-hoc committees have generally not been necessary to govern RTIIS effectively. The principal function of the governance committee is to approve applications from new member agencies for participation in RTIIS.

The governance structure, and basic terms and conditions of participation in RTIIS, are established in a straightforward Memorandum of Agreement (MOA), which is included as Appendix A (see page 21). The MOA is relatively simple and brief, but addresses the principal concerns of participating in RTIIS. It states the purpose and intended benefits of the partnership and establishes the process that members follow to join and, if necessary, withdraw their participation. The agreement addresses issues of confidentiality, liability, and indemnification, and clearly establishes that information ownership remains with the original agency. It also defines the process by which agencies and their staff gain access to the system after joining the partnership.

The Solution: Features

The basic functionality of RTIIS is to receive regular information

extracts from various information sources in Los Angeles County, convert each extract to a common format and structure, and store the information in a database that users access via a sophisticated but user-friendly interface. The user interface allows users to create queries across some or all the information sources, to include several key investigative variables in those queries, and to view results in a tabular or map-based format. RTIIS includes RMS information from all 45 municipal partner agencies.

The basic unit of information in RTIIS is a document, from which specific pieces of data are extracted to index the document. Everything in the system ties back to a document—such as an arrest report, incident report, citation, field interview, or warrant. As an example, if an incident report ties together three individuals (two subjects and one witness), a weapon, and a vehicle, COPLINK will extract identifying information from each segment of the report, and then associate the report with that identifying information.

The document index supports subsequent information retrieval and analysis in two ways. First, if officers know a specific piece of information, such as a person's name or a vehicle's license plate number, they can search the repository for any documents matching that specific information. The results consist of a list of matching documents that the user can select for viewing (Figure 2).

IRIS Leads Deputies to Male Flasher

On February 26, 2009, deputies at the LASD's Crescenta Valley Station took a report that stated a 19-year-old female was the victim of repeated incidents of indecent exposure by an adult male living in her condominium complex. The incidents took place between July 2008 and February 2009.



Using IRIS, an LASD Crime Analyst was able to identify a possible suspect based on previous incidents at the location (none related to indecent exposure). The possible suspect's name and photo were given to the investigating detective, who matched it to the description given by the victim. The victim positively identified the suspect from a photo lineup.

COPLINK Training Class Exercise Helps ID Suspect

A gang detective with LASD Operation Safe Streets took the COPLINK class in March 2008. During the class, he was able to do dry runs on active cases and thought he had found a second suspect in a robbery investigation.

The system provided the second suspect through a “moniker” search. According to the detective, “This suspect had already timed-out in CalGang® [a statewide gang member database], so I couldn’t get an identity on him. I proceeded with the information provided by COPLINK. The suspect turned out to be a parolee. I interviewed him and...he self-admitted to the robbery. He was just sentenced to two years in state prison.”



Person Details
BABYCAKES, CHRISTOPHER D **DOB: 02/17/1981**

LOCAL ID: [REDACTED]
 ID: [REDACTED]
 FBI: [REDACTED]
 SEX: M HAIR: Brown HT: 408-511
 RACE: White EYES: Brown WT: 65-185

ALIASES

NAME	DOB
BABYCAKES, CHRIS	02/17/1981
CARDENOS,	02/17/1981
CARDENOS, X	02/17/1981
NOTLIN,	02/17/1981
NOTLIN, X	02/17/1981
PETHERICK,	02/17/1981
PETHERICK, X	02/17/1981
POSTRZECH, CHRIS	02/17/1981
POSTRZECH, JOHNEYE	02/17/1981
POSTRZECH, JONATHAN	02/17/1981

DOB

DOB	COUNTRY	STATE
02/17/1981		

DEMOGRAPHICS

	SEX	RACE	ETHNICITY	COMPLEXION	BUILD	DATE
1	M	White		Fair	Thin	09/17/2000
2	M	White		Fair	Medium	08/16/2000
3	M	White		Medium	Medium	04/17/2000
4	M	White		Medium	Medium	03/10/2000
5	M	White		Light	Thin	03/15/2000
6	M	White	Hispanic	Medium	Thin	02/07/1999
7	M	White	Hispanic	Fair	Thin	06/04/1999

SEARCH FOR

Basic Search Refined Search

Search For:

- Person
- Organization
- Location
- Place
- End
- Vehicle
- Firm
- Property
- Security
- Document

Associated With:

Remove Reset

Full Path

Find Associations

Return Visualizer Results

Figure 2: COPLINK Person Details Screen
 (Screen shot shows fictitious person from COPLINK training database)

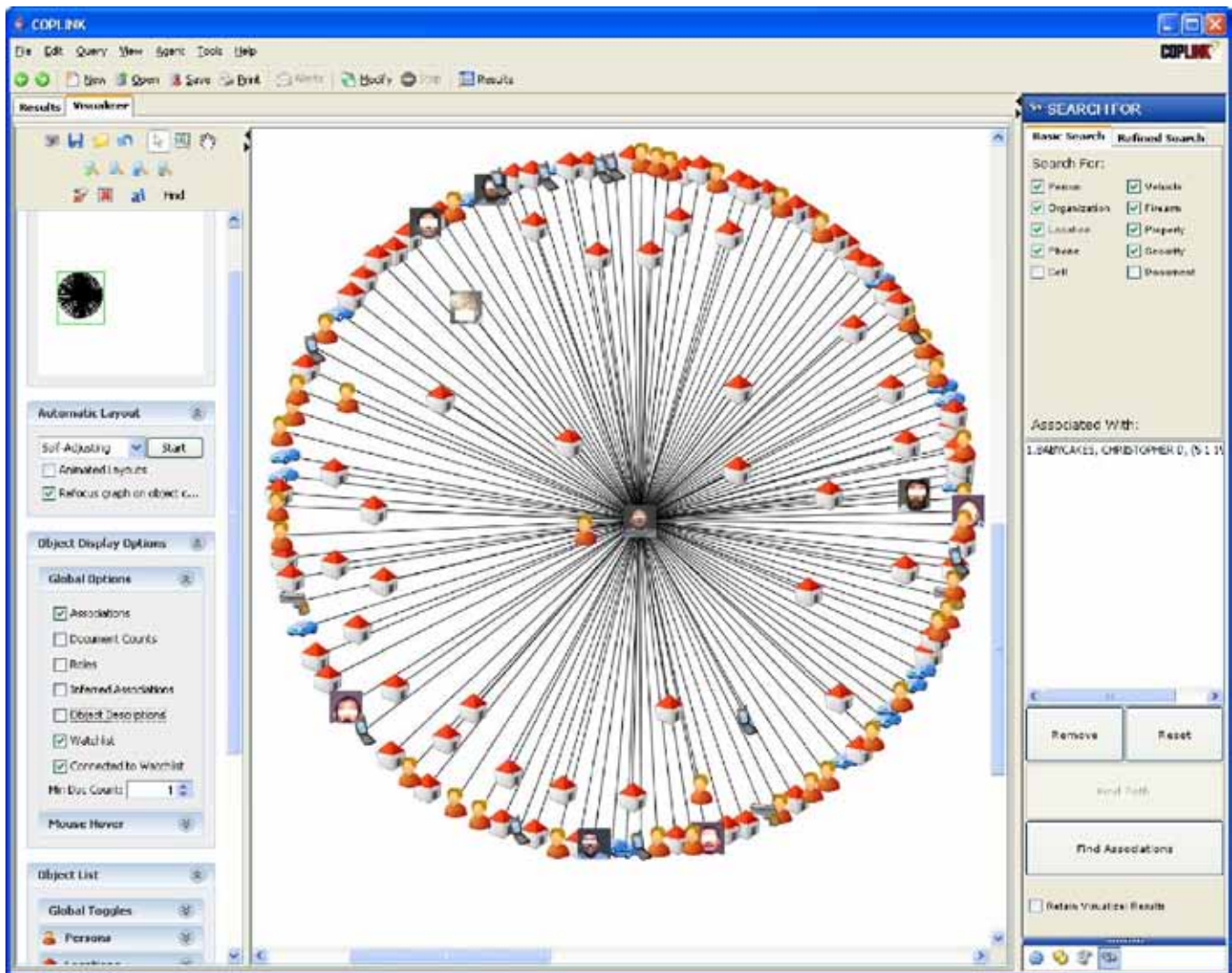


Figure 3: COPLINK Link Analysis “Hub and Spoke” Display

In addition to simple searches for matching documents, RTIIS provides sophisticated “link analysis” that uncovers relationships and linkages across information sources from different jurisdictions, that would be very difficult to detect manually. The

user interface displays the links in an intuitive “hub and spoke” display that shows objects and their relationships (Figure 3). This allows officers to follow leads and “drill down” into areas as their investigation proceeds.

LASD and LAPD share their information via separate COPLINK nodes; the other 45 partners share via a single COPLINK node for RTIIS. In addition, a COPLINK node with information from 23 law enforcement agencies in Orange County (which borders Los Angeles County to the southeast) connects to RTIIS, making the two counties' information available transparently to one another.

RTIIS also provides a single interface to Federal partner information repositories, including the U.S. Department of Justice OneDOJ system, the FBI N-DEx system, and the U.S. Immigration and Customs Enforcement Pattern Analysis and Information

Collection (ICEPIC) system of the Department of Homeland Security. RTIIS significantly reduces the overall county cost of contributing to these national repositories by leveraging the common information format of RTIIS and a single reporting point to the Federal partners. Small agencies in the county, in effect, gain the benefits from participating in these national initiatives at no extra cost, since the interfaces were developed once and shared across all participating partners.

This diagram (Figure 4) depicts the information sources connected through RTIIS.

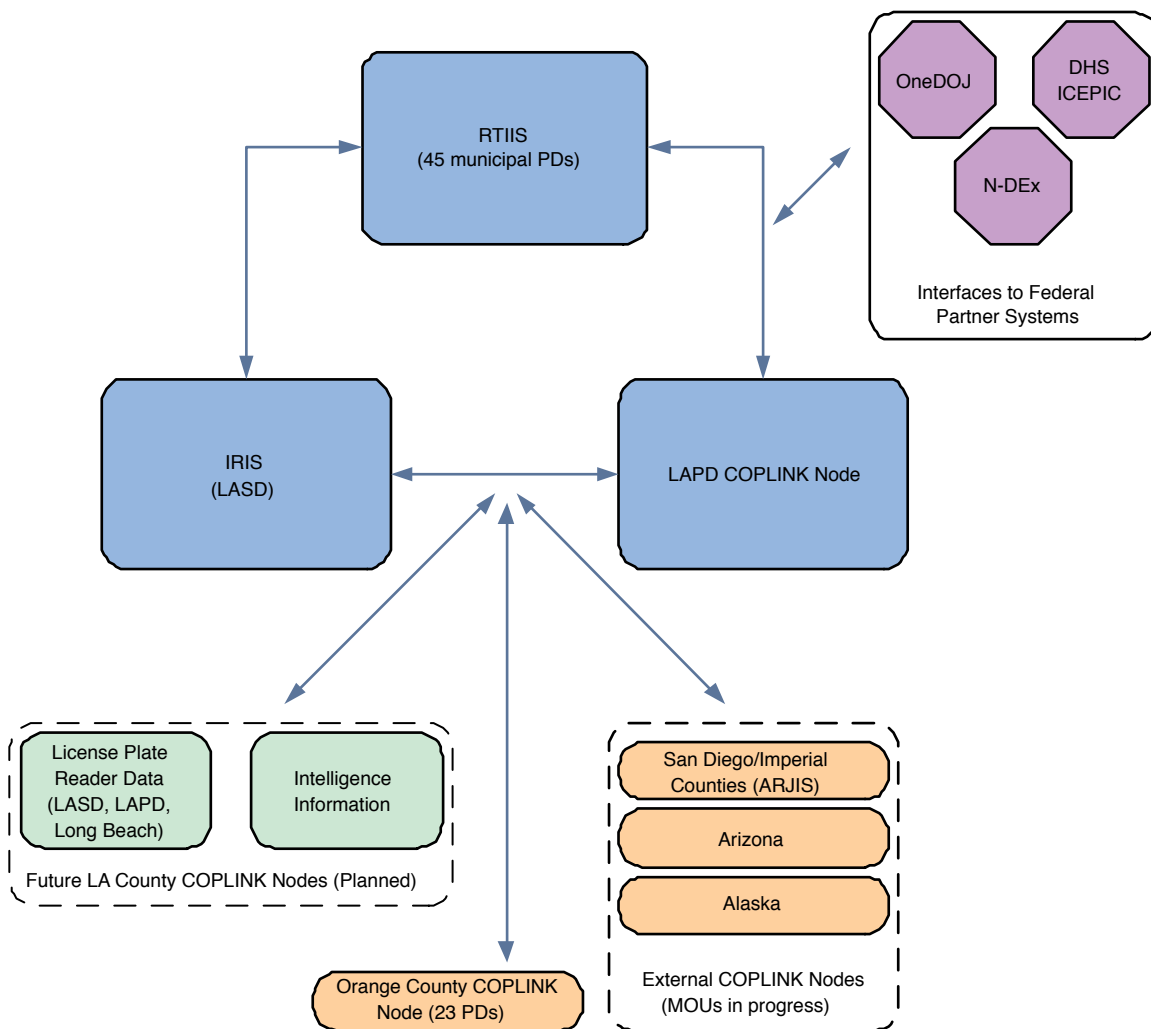


Figure 4: Information Sources Connected Through RTIIS

RTIIS supports five basic query parameters, and across these search types, the system fulfills nearly 750 queries per day on average.

Query type	Average number of queries per day
Person of interest (search by name, identifier, identifying marks/tattoos, etc.)	570
Vehicle (partial or full license plate, make/model/color, etc.)	72
Phone number	57
Location	31
Organization name	5

IRIS, via N-DEx, Provides North Las Vegas PD with Critical LASD Information

In October 2008, the North Las Vegas Police Department (NLVPD) received information from its Problem Solving Unit (PSU) that a person was selling narcotics at an address in Las Vegas and that he possibly had handguns in the residence as well.

The Department was only given the moniker "Beagle,"* that he was a gang member from California, and that a black female also lived with him. An investigator with the department's Special Operations Division reported that he "used every database I had available to me: SCOPE, OffenderTrak, NCIC, Lexis/Nexis, GangNet, CalGang and our CADS, but could not locate a match based on the limited information."

A utility subpoena showed the name of "Jane Smith" and a reference listed her husband as "James Roe." The investigator was able to

locate "James Roe" through the CalGang database; however he had a different moniker listed and the physical description did not match the NLVPD's information. After exhausting all his resources, the investigator asked that the woman's name be run through N-DEx. This resulted in information about a call for service in California with her name listed as one of the parties involved. Further investigation showed a male associate involved in that call was a gang member named "Edward Suspect." Since the NLVPD had information that "Beagle" was a gang member, the investigator ran the name "Edward Suspect" through the CalGang database; the results listed him as a gang member out of Watts, California, with the moniker of "Beagle."

The investigator was then able to run the name "Edward Suspect" through NCIC, which returned an extensive criminal history, as well as a felony warrant for possession of a stolen vehicle. Suspect's criminal history included

attempted murder, resisting a police officer, and sexual assault of a victim under age 14. While looking at Suspect's personal information, the investigator noticed he used an AKA of James Roe. His photo and information were given to officers serving the warrant.

The warrant was served on Edward Suspect, who initially identified himself as James Roe. After being confronted with the information that the NLVPD had obtained from IRIS via N-DEx, he admitted his real name and said he lied because he knew he had a felony warrant and would be going to prison for a long time. The warrant resulted in the recovery of 71.9 grams of rock cocaine, 3.3 grams of marijuana, 90 rounds of ammunition, 2 handguns, and \$950 cash. Without the help of N-DEx, Edward Suspect would have been booked as James Roe, with no identification, and possibly been released before his true identity was revealed.

**Identifying information about suspects has been changed throughout this case study.*

Security and Privacy

Information security and protection of citizens' privacy rights is of paramount importance to successful law enforcement information sharing projects. A combination of technology and policy ensures that RTIIS fulfills the security and privacy requirements of the Los Angeles County partners.

All interaction with the COPLINK nodes in RTIIS—both for submission of information from agencies and fulfillment of queries from users—occurs over the private, secure Los Angeles County law enforcement information sharing network. This network, called **PAC-50**, existed prior to implementation of RTIIS, and so was a natural choice for the deployment of RTIIS. LASD manages the PAC-50 network on behalf of the county law enforcement community. The use of a secure private network ensures the security of RTIIS information in transit between agencies.

User access to RTIIS relies upon COPLINK's built-in user authentication capabilities. Each participating agency has an Agency System Administrator who is authorized to create user accounts on the RTIIS COPLINK node. The MOA establishes the responsibilities of a system administrator, including ensuring that users have a legitimate purpose for accessing the system and that users have acknowledged, via signature, that they agree to abide by the terms and conditions of access to the system. System

administrators are responsible for terminating the accounts of users who leave their agency or otherwise are no longer authorized to access RTIIS information.

The RTIIS authorization model is group-based, allowing Agency System Administrators to place users in groups based on their need to access certain types of information. In its initial implementation, RTIIS has employed a fairly simple three-level classification:



“White” information is available for full viewing by any authorized user of the system.

“Grey” information is a query result in which the system informs the user that there is information matching the query parameters, but the information is only available by contacting the original agency rather than through RTIIS itself.

“Black” information is excluded from user access, but if a user executes a search that matches, the original agency is notified of the user's interest.

COPLINK maintains logs of all user activities in RTIIS, and the MOA requires participating agencies to keep activity logs for a period of three years.

All of the information in RTIIS is public information extracted from police reports, traffic citations, and dispatch records. The system does not collect personally identifiable information other than what already appears in these public sources. The RTIIS information sharing agreement states the purpose for which the database exists and establishes who has access to the system. While RTIIS is used by investigators and analysts to build criminal cases, the RTIIS database itself does not contain intelligence as defined by 28 CFR Part 23.



Technology: How it Works

The RTIIS solution follows a centralized or *data warehouse* model of information integration (Figure 5). In this model, information from each participating agency is extracted from that agency's local systems, transformed into a standard format, and submitted to a central database. A centralized application connects to the central database (not individual agency systems) to provide users with query and analysis features. (This approach is not the only way to provide query access to multiple agencies' data; Appendix B (see page 27) discusses an alternative approach and the advantages of each.)

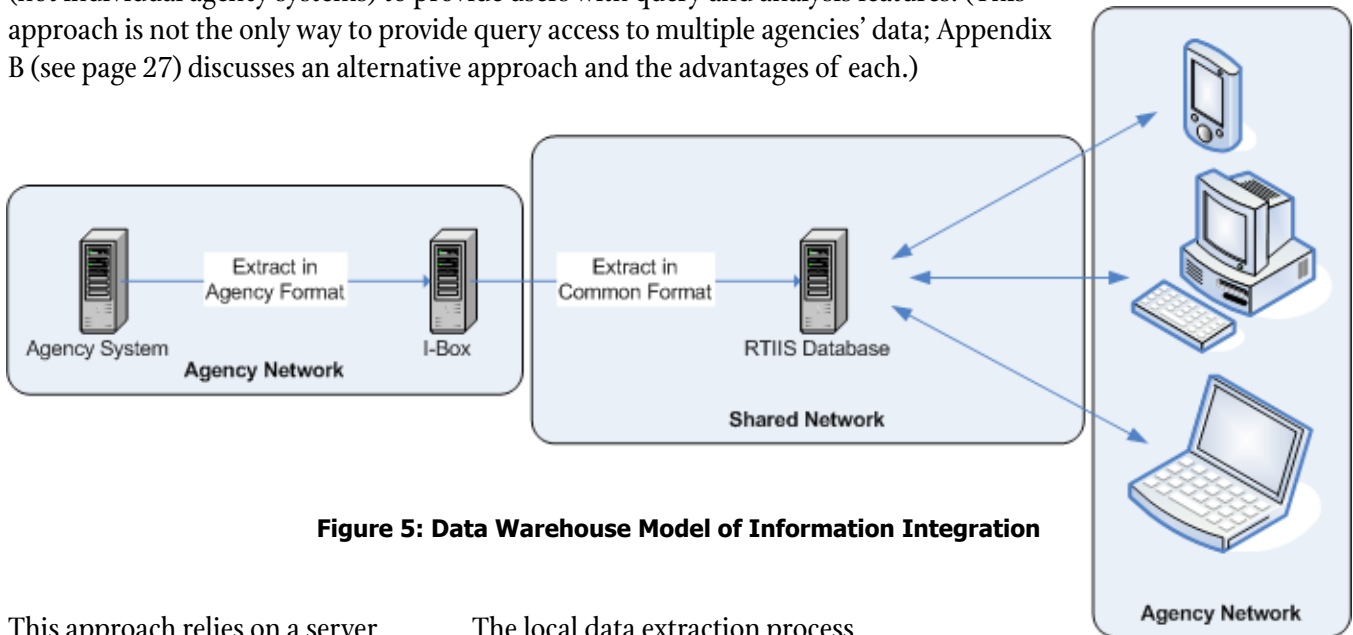


Figure 5: Data Warehouse Model of Information Integration

This approach relies on a server and software that reside at each agency and extract data from agency systems on a periodic basis. For RTIIS agencies, the software consists of a standard COPLINK component, called I-Box, that was configured and customized during deployment of the solution. The nature of this configuration depends on the specific systems in use within the agency; if KCC has configured I-Box for a particular system in another jurisdiction, then the configuration will likely be easier than if the system is a locally-developed custom application. In every agency, however, the configuration process involves consulting with records personnel and other subject-matter experts to ensure that the mapping from local agency data to standard data is accurate.

The local data extraction process accommodates a diversity of techniques for extracting agency data. Across the RTIIS participating agencies, the two most common techniques are *direct database access* (in which I-Box performs queries directly in an RMS's database) and *file extracts* (in which I-Box reads a file of data produced by the RMS).

Users interact with RTIIS via an application that loads in an ordinary web browser. The application leverages Java technology,⁶ allowing it to run seamlessly on most users' workstations.

⁶ Java is a programming language and software development platform governed by a consortium of technology companies led by Sun Microsystems. Software developed in Java runs seamlessly on a variety of computer hardware and operating systems.

Communications between the I-Box servers in each agency and the central database, as well as queries between users' workstations and the database, travel over an ordinary TCP/IP network. For RTIIS, data traverses the county's secure private law enforcement network, which was in place prior to deployment of RTIIS. COPLINK can also leverage the Internet and semi-private networks (such as government networks) as long as they are secured with virtual private network (VPN) technology.

User Training: A Key Element of the Solution

With any technology tool, effective user training is an important component of a successful deployment. Users cannot be effective or efficient without understanding the features of a system and how to use the system in the context of their daily work. The RTIIS training program, led by LASD staff, addresses this need by providing users from the participating agencies with robust training on the features and operation of COPLINK.

LASD Sergeant Tab Rhodes, who oversees the RTIIS training program, explains that the training focuses on objectives beyond just the mechanics of using the query interface. “We try to bring officers from different jurisdictions together in the same class, to emphasize the county-wide and multiagency approach of RTIIS,” he says. “In the training demonstrations, we ask participants to bring real, current cases, and show how investigators can use the system to find relevant information. Several times, training sessions have revealed subjects or incidents familiar to participants who previously had not been in contact. That kind of experience clearly shows the power of the technology and the relevance of sharing across jurisdiction boundaries.”



Sergeant Rhodes also uses the training to demonstrate the importance of capturing accurate and complete information at the source. When electronic incident reports and field interviews lack subject descriptive data, location information, or detailed description of the circumstances, there is less information for the system to use in identifying links, and fewer pieces of data for queries to match. Where previously such information may have gone unused—and therefore was not worth collecting—the training emphasizes that it will now not only be used, but also will be crucial to the maximum effectiveness of RTIIS.

To accomplish these objectives, LASD staff found that they needed to enhance the basic training materials that KCC provided. These stock materials focus mostly on the operation of the tool, and not the “softer” skills of collaboration and information capture. They also do not include specific examples or cases from the participating jurisdictions, since they are intended for use nationwide. Early in the project, the RTIIS partners decided to create a specialized training program that accomplished these additional goals.

Parolee Steals Cell Phone from Girl at Bus Stop, Gets Nabbed by IRIS

In November 2008, the LASD's Compton Station requested help in the identification of a robbery suspect. The suspect had stolen a cell phone from a girl at a bus stop in August 2008 and had logged onto the stolen phone with an AOL Instant Messaging (AIM) account. When the victim was issued a new phone, the telephone company downloaded the stolen phone's information, which included the AOL logon by the suspect. The victim then engaged in phone-to-phone messaging with the suspect—eventually, the suspect told the victim he was a Crips gang member and threatened to kill her.



A researcher in the LASD's Commercial Crimes Bureau Detective Information Resource Center (DIRC) was given the suspect's e-mail address, from which a My Space.com account was located, along with five photographs of the suspect. Using IRIS, and by searching only on Race, Sex, Astrological Sign, and a Tattoo, the suspect was positively identified and found to be on active parole through the California Department of Corrections for burglary. With the help of his parole officer, the suspect was arrested and is being charged for a parole violation on top of the cell phone robbery. The suspect had stolen the phone on August 20. When he was arrested on December 4, he was carrying the stolen cell phone in his pocket.

Future Plans

The RTIIS partners plan to continue improving upon the current system. In addition to any improvements in the technology that KCC may provide, the partners themselves envision implementing the following new capabilities:

- Continue to incorporate more agencies' data into the system; LASD is leading an effort to execute a statewide law enforcement sharing agreement and establish a statewide license to COPLINK.
- Deploy to mobile data computers for agencies that have (or will obtain) them.
- Develop enhanced geographic information capabilities and integrate with other geographic information sources.
- Increase strategic use of the information in RTIIS by developing regional analytical tools and leveraging the information for countywide planning.
- Finalize a privacy policy for RTIIS. (Development of the policy is underway.)

Lessons Learned

The RTIIS initiative in Los Angeles County offers several lessons learned for other partnerships considering implementing similar solutions.

Establish representative governance and partnership. For a multiagency information sharing initiative to succeed, it is important that decisions take into account the diverse interests and perspectives of all the participants. Ensuring that all voices are heard helps make sure that the resulting system is the best fit to the needs of users, and that all agencies are "bought into" the solution. An effective mechanism for bringing all perspectives to the table is to establish representative governance, in which the participating agencies select a subset of their peers to make decisions. The governance structure, along with other expectations and responsibilities of the partners, should be established in a formal information sharing agreement that is executed by each partner as a condition of participation.

Leadership is important. Equal in importance to forming a representative governance structure is ensuring that one partner is capable of taking a leadership role in implementing the information sharing solution. The lead partner must have the technical expertise, business knowledge, and project management ability to lead the project forward. Leadership also requires the confidence and trust of the partners in the lead

agency's ability to deploy technology, manage vendors, facilitate decision-making, and advocate for broader adoption of the solution.

Create a culture of information sharing. A successful consolidated data repository like RTIIS requires that front-line officers collect high quality, accurate information, and enter this information into their local systems so that it can eventually migrate into the central data warehouse. Sometimes patrol officers and deputies and their supervisors resist robust information capture because traditionally little use has been made of the data. As such, they fail to see the value returned for the extra effort expended.

Demonstrating the impact of capturing detailed information is essential to changing this viewpoint, if it exists. Technology like RTIIS shows how detailed information leads directly to better analysis and a greater ability to solve crimes. In addition, it is important for officers and deputies to recognize that they are truly part of a regional law enforcement partnership that strives to eliminate information sharing barriers between jurisdictions. In Los Angeles County, the RTIIS user training program has been an essential mechanism for creating the necessary information sharing culture.

Incorporate real cases into the training. The RTIIS partners have found that trainees benefit the most from seeing the power of the technology to help them solve real cases. This is best accomplished by having participants bring queries from real investigations—either ongoing or recently completed. Using examples that are relevant to a trainee's current work helps the lessons of training stick. And LASD has found that in many cases, participants in the same class can find links in these example cases that cross their jurisdictional boundaries, further emphasizing the regional focus on crime fighting that the solution is intended to foster.

Market the solution through success stories. LASD, as the coordinating partner in RTIIS, makes an effort to collect stories from users that demonstrate how RTIIS has helped them in their work. These stories (some of which have been included throughout this case study)

prove valuable in advocating for additional participation and funding. They are also useful in the training to motivate interest from new users.

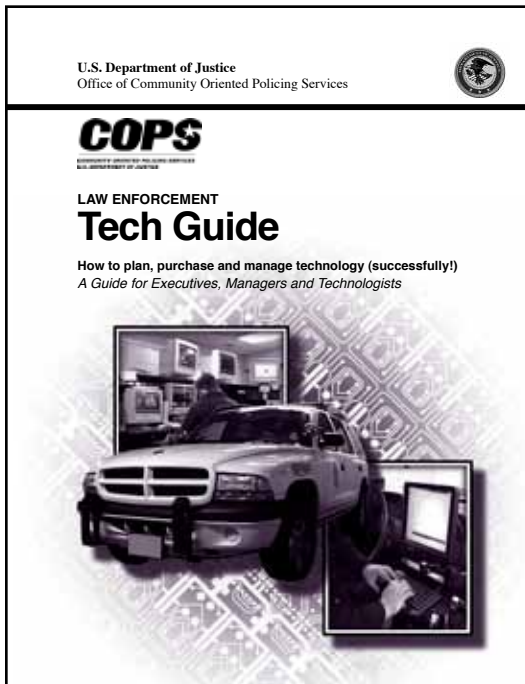
Plan to deal with outside sharing requests. Stakeholders from outside a partnership will sooner or later express an interest in gaining access to the repository to assist in their own investigations. Federal agencies and agencies in other states are common examples that have arisen with RTIIS. The Los Angeles County partners discovered, once access requests started coming in, that their information sharing agreement did not provide a mechanism for handling them. Information sharing partnerships should anticipate that others will appreciate the value of their data and will eventually request access. The partners should discuss and agree upon a process for dealing with such requests, and establish the process in their information sharing agreement.

IRIS Leads Deputies to Graffiti Vandal

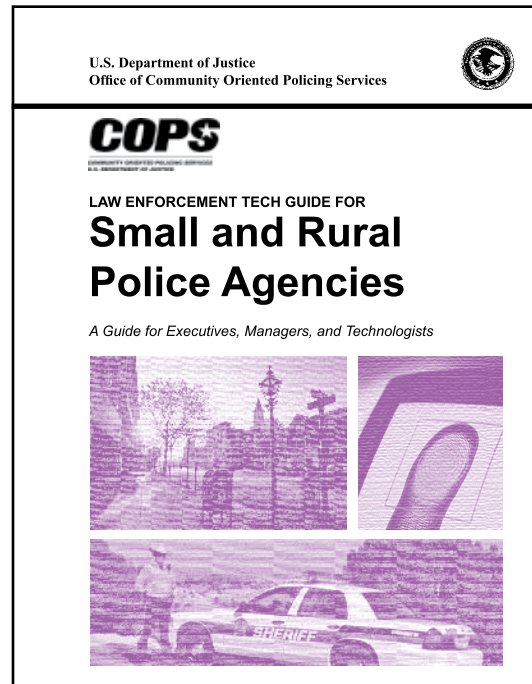
In June 2008, the LASD Transit Services Bureau received a video of someone marking a train on the Metro Green-Line with the moniker of "Cargo." A Transit Bureau detective typed "Cargo" into IRIS, among other search criteria. Of the hits he found, one contained a photo that matched that of the suspect on the video.

A Special Problems Unit deputy was sent to investigate and found vandalism near the suspect's home and on his property. He also found other damage matching the suspect's tag name on the Metro System. A search warrant was written and served on the suspect, who was taken into custody. Deputies found several pieces of evidence, including tagging exemplars.

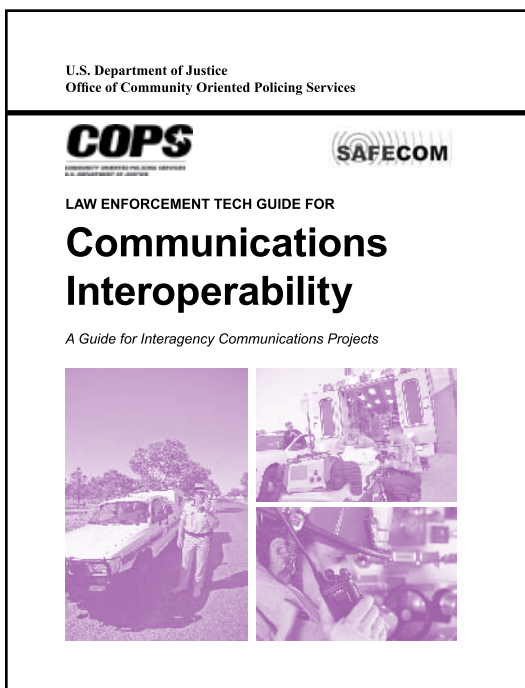
Many of these lessons reflect general best practices of technology implementation, which are addressed in the following publications from SEARCH and its U.S. Department of Justice partners:



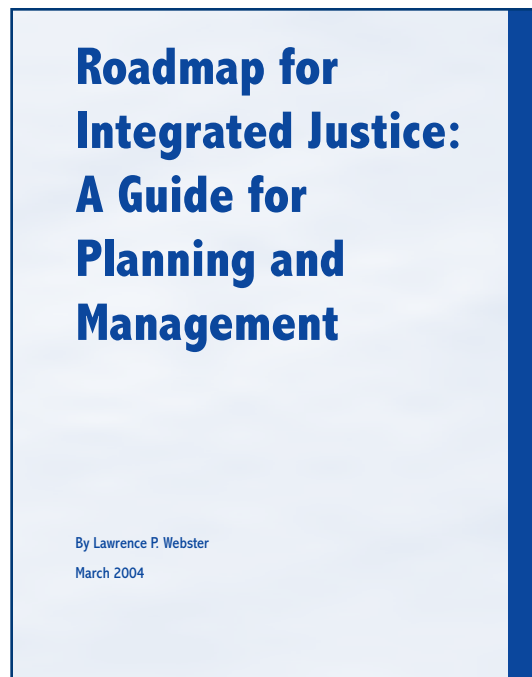
<http://www.search.org/files/pdf/TECHGUIDE.pdf>



<http://www.search.org/files/pdf/SmallRuralTechGuide.pdf>



<http://www.search.org/files/pdf/ComminteropTechGuide.pdf>



<http://www.search.org/files/pdf/StrategicRoadmap.pdf>



The partner law enforcement agencies in Los Angeles County recognized the importance of a regional, information-led approach to combating crime. They established a partnership to implement the vision of a data repository that consolidates information from their individual agency systems. They formalized the partnership in an information sharing agreement and governance structure, and have invested in a training program that not only teaches users the mechanics of using the system, but also fosters a culture of information sharing in the partner agencies. They have deployed innovative, industry-leading technology to fulfill the vision. And ultimately, they have a growing library of success stories that demonstrate the power of the solution.

SEARCH hopes that this case study is of value to law enforcement agencies who have a similar vision and are considering the implementation of a similar solution. Through support from the U.S. Department of Justice, Bureau of Justice Assistance, SEARCH is available to assist the law enforcement community with planning, designing, implementing, and governing information sharing solutions. Contact us at sgi@search.org for more information.

SEARCH acknowledges the contributions of staff from the Office of Los Angeles County Sheriff Leroy D. "Lee" Baca, including: Captain Scott Edson, Lieutenant Chris Cahhal, Sergeant Tab Rhodes, and Mr. Meng Chua. Their sharing of information in personal interviews and follow-up emails have been essential to the completion of this case study.

**MEMORANDUM OF AGREEMENT
FOR THE
LOS ANGELES REGIONAL INTEGRATED LAW AND JUSTICE PROJECT
AMONG THE
REGIONAL TERRORISM INTELLIGENCE AND INTEGRATION
SYSTEM PARTICIPATING AGENCIES**

I. OVERVIEW

- a. **Background:** The mission of the Los Angeles Regional Integrated Law and Justice Project (“LARILJP”) is to coordinate the development and implementation of a regional justice information sharing system that will allow law enforcement agencies throughout Los Angeles County to share information in their case and records management systems. The goal is to protect the total community by efficiently and effectively providing accessible, accurate information for the speedy investigation and apprehension of terrorists and other law violators. The sharing of information shall be achieved through the COPLINK System (“COPLINK”). A “Contractor” (currently Knowledge Computing Corporation) shall install and maintain COPLINK.
- b. **Intended Benefits:** By sharing public safety information, LARILJP participating agencies (“Agencies” or “Agency”) will be able to improve their responses to terrorism and community crime. COPLINK provides sophisticated analytical tools that will allow authorized users to discover links and relationships by providing consolidating data across Los Angeles County. This will allow Agencies to solve previously “unsolvable” incidents and investigate serial criminal activity.
- c. **Purpose:** The purpose of this agreement (“Agreement”) is to outline conditions under which the Agencies will share and use information in COPLINK. By signing this Agreement, Agencies, as well as all individuals who operate or use COPLINK, agree to adhere to the guidelines specified in this Agreement.
- d. **Agency Participation:** The LARILJP is a cooperative venture of justice agencies in Los Angeles County, California. Any law enforcement agency in Los Angeles County may apply to participate in LARILJP. To participate in LARILJP and have access to COPLINK, an Agency applicant shall apply to the LARILJP Governance Committee by submitting a proposal that outlines its intended use of COPLINK, the type of data it intends to contribute, and any other information requested by the Governance Committee. A simple majority vote of approval of the Governance Committee is required to approve an Agency’s participation in COPLINK. Once approved, each Agency will proactively cooperate with other participating Agencies, the Contractor, and its own system vendors and/or maintenance contractors to facilitate:
 1. Network access and connectivity
 2. Data extracts for engineering and testing purposes
 3. Production extracts
 4. Required modifications to their source systems
 5. Regular data updates as agreed to during the design process
 6. Timely review and approval of design documents and test results
- e. **Agency Withdrawal:** An agency may withdraw from participation in COPLINK at any time by providing written notice to the LARILJP Governance Committee. If any Agency wishes its data withdrawn from COPLINK, the withdrawing Agency shall contact the Contractor and request data removal. The withdrawing Agency is responsible for the cost associated with the removal of its data from COPLINK.

II. AUTHORIZED RELEASE OF INFORMATION

- a. Sharing of Information: Each Agency authorizes the release of information residing in its records management system to all users of COPLINK as permitted by law. It is the responsibility of each Agency to specify which data to share, as well as any special requirements that may apply to certain kinds of information. An Agency that does not want certain data made available from its records management system to COPLINK is responsible for ensuring that the data is not included in data transfer to COPLINK. An Agency that wants data from its records management system to be made available only to a select group of COPLINK users is responsible for placing the appropriate restriction indicator on the underlying data in the agency's internal records management system or database.

California law prohibits the release of victim information in specific sex related crimes, sealed juvenile records, and the release of summary criminal history to unauthorized persons.

- b. Limitation on Information Sharing: Information contributed by each Agency shall only be shared with or released to those Agencies that have entered into this Agreement. Only authorized Agency employees who have an approved login and password ("Authorized Users") will be allowed to access or use information in the COPLINK System.
- c. Liability: Each Agency is solely responsible for any and all liability, claim, administrative proceedings, losses, expenses or any injury, including death, or damage of any kind whatsoever, whether actual, alleged or threatened, including actual attorney fees, court costs, interest, defense costs and expenses associated therewith, including the use of experts, and any other costs of any nature without restriction incurred in relation to, as a consequence of, or arising out of the Agency's use of the COPLINK system and /or its performance under this Agreement.
- d. Indemnification: Each Agency executing this Agreement is a public entity. In contemplation of the provisions of Section 895.2 of the Government Code of the State of California imposing certain tort liability jointly upon public entities, solely by reason of such entities being parties to an Agreement as defined by Section 895 of said Code, the Agency parties hereto, as between themselves, pursuant to the authorization contained in Section 895.4 and 895.6 of said Code, will each assume the full liability imposed upon it or upon any of its officers, agents, or employees by law, for injury caused by a negligent or wrongful act or omission occurring in the performance of this agreement, to the same extent that such liability would be imposed in the absence of Section 895.2 of said Code. To achieve the above-stated purpose, each Agency shall indemnify, hold harmless, and defend each other, and the officers, agents and employees of each other, from and against any and all liability, claims, administrative proceedings, losses, expenses, or any injury, including death, or damage of any kind whatsoever, whether actual, alleged or threatened, actual attorneys fees, court costs, interest, defense costs and expenses associated therewith including the use of experts, and any other costs of any nature without restriction incurred in relation to, as a consequence or, or arising out of the performance of this Agreement, including the use or alleged or actual misuse of the COPLINK system by the Agency and its employees. The provision of Section 2778 of the California Civil Code is made a part hereto as if fully set forth herein. Each Agency executing this Agreement certifies that it has adequate self insured retention of funds to meet any obligation arising from this Agreement.
- e. Internal Audit: Each Agency shall name a System Administrator, who shall conduct an internal audit on a periodic basis to ensure information is reasonably up to date and user queries are made for legitimate law enforcement purposes. COPLINK will require each Authorized User to input the reason for the requested information before any information is generated. This information shall be recorded on COPLINK, and retained to allow the System Administrator to complete the internal audit.

APPENDIX A

Information Sharing Case Study: Los Angeles County, California

III. INFORMATION OWNERSHIP

- a. Ownership: Each Agency retains control of all information it provides through COPLINK. Each Agency is responsible for creating, updating, and deleting records in its own records management system or database, according to its own policies. Each Agency shall use its best efforts to insure the completeness and accuracy of its source data.
- b. Unauthorized Requests: Requests for information in COPLINK that are not authorized for viewing will be referred to the Agency that authored or originated the requested information (“Source Agency”).
- c. Prohibition Against Release of Information: No Agency or Authorized User shall release or make available any information it has accessed to any person or entity not authorized to access the COPLINK system, or to any third party without the prior written approval of the Source Agency, or as required by law.
- d. Public Record Requests, Subpoenas and Court Orders: Any Agency receiving a public records request, subpoena, or court order (“Legal Request”) for information in COPLINK authored by or originated by another Agency shall respond to the Legal Request, and shall immediately provide a copy of the Legal Request to the Source Agency System Administrator.

IV. UNDERSTANDING ON ACCURACY OF INFORMATION

- a. Accuracy of Information: Agencies agree that the data maintained in COPLINK consists of information assumed to be accurate. Agencies will participate in several testing sessions, to validate and ensure that its information is accurate. However, data inaccuracies can arise for multiple reasons (e.g., entry errors, misinterpretation, outdated data, etc.). It shall be the responsibility of the Agency requesting or using the data to confirm the accuracy of the information with the Source Agency before taking any enforcement-related action.
- b. Timeliness of Information: Each Agency shall determine the frequency with which its data will be refreshed in COPLINK. In addition, each Agency has its own policy regarding the speed at which incidents are recorded in its internal records management systems. Since changes or additions to data do not get updated in COPLINK on a real-time basis, Agencies recognize that information may not always be timely and relevant. It shall be the responsibility of the requesting Agency to confirm the timeliness and relevance of the information with the Source Agency. Additionally, a data refresh schedule will be published by each System Administrator to enable a user to determine the potential timeliness of each Agency’s data.
- c. Hold Harmless: To the extent permitted by law, Agencies agree to hold Source Agencies harmless for any information in COPLINK, or any action taken as a result of that data, regardless of whether the data is accurate or not, or any time delay associated with changes, additions, or deletions to the information contributed. This hold harmless provision shall not apply to the willful misconduct or gross negligence of Source Agencies.

V. USER ACCESS

- a. Login Application Process: Each Agency’s System Administrator is responsible for management of user accounts at that Agency. Each Agency agrees that all Authorized Users shall be current employees and be authorized to review criminal history data for legitimate purposes. Each potential user shall submit a request for a login and password to the Agency System Administrator. The Agency System Administrator shall have discretion to deny or revoke individual access.

- b. Login Assignment: Each Authorized User will be issued a user login and a default password by the Agency System Administrator. Upon logging into COPLINK for the first time, each Authorized User will change the default password to another password. Authorized Users may be assigned to groups that have different levels of access rights based on the level of restriction of the information.
- c. Provision of Agreement: The Agency System Administrator must provide a copy of the terms and conditions of this Agreement to all Authorized Users when they are issued a login ID for the system. Each Authorized User shall sign an acknowledgement stating, "I have received a copy of the terms and conditions of usage of COPLINK. I agree to comply with the terms and conditions and I understand that violation of the terms and conditions may lead to disciplinary action and/or criminal prosecution." The Agency System Administrator shall maintain the signed acknowledgements at all times.
- d. Intended Use: Each Authorized User agrees that COPLINK, the information contained in it, and the networking resources it provides are to be used solely for purposes consistent with the mission of the LARILJP. Authorized Users acknowledge that the information in COPLINK will be shared and used for authorized purposes only as permitted by law. Authorized Users shall not use or share the information for any unethical, illegal, or criminal purpose.
- e. Limitations on Use of Logins: An Authorized User may not access COPLINK by using a name or password that was assigned to another user. An Authorized User cannot give his or her password to another person, including another user, to access the system.
- f. Audit Trail: Each transaction on COPLINK is logged, and an audit trail is created. Each Agency System Administrator shall maintain the audit trail for a minimum of three years. Requests for transaction logs shall be made in writing by the Agency System Administrator, who shall provide the logs to the requesting party within a reasonable amount of time.
- g. Termination of Logins: Each Agency System Administrator is responsible for timely removal of any login accounts as Authorized Users leave the Agency, fail to meet the requirements of this Agreement, or are denied access by the Agency System Administrator for any other reason.

VI. CONFIDENTIALITY OF INFORMATION

- a. Information Confidentiality: Information in COPLINK is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information in COPLINK. The information will otherwise be kept confidential.
- b. Internal Requests for Information: An Authorized User who receives a request from a non-authorized requestor for information in COPLINK shall not release that information, but may refer the requestor to the Source Agency.
- c. Removal or Expungements of Records: LARILJP shall determine a schedule for record deletion, removal, expungement, and other edits. Any Agency that seeks to edit a record sooner than the scheduled time shall contact the Contractor directly and arrange for the change to be manually processed.

VII. SYSTEM ACCESS

- a. Network Access: Access to COPLINK will be provided by a private network maintained by the Los Angeles County Sheriff's Department or any other secure network configuration that is mutually acceptable to the member agencies.
- b. System Availability: COPLINK shall operate 24-hours a day, 7-days a week, with downtime limited to those hours required for any necessary maintenance activities.

VIII. AGREEMENT TERMS

- a. Term: This Agreement will commence on the date that it is adopted by the first LARILJP participating Agency, and shall last until the last Agency withdraws, pursuant to section I. e. of this agreement.
- b. Changes to Agreement: Additional law enforcement agencies may be added to LARILJP by signing an amended copy of the Agreement, accepting its terms and conditions, and obtaining an approval by a simple majority of the LARILJP Governance Committee. Based on ongoing monitoring of COPLINK, Agencies may propose other changes to this Agreement. Such proposals require the approval of a simple majority of the participating Agencies.
- c. Supplemental Policies: An Agency may add individual guidelines for its own computers or networks providing they do not conflict with the provisions of this Agreement.
- d. Sanctions for Non-Compliance: Any Agency that violates the guidelines of this may be disconnected from the COPLINK System. The Agency will be provided with a 60-day written notice of the violation, and the opportunity to correct the violation. Failure to meet the guidelines will result in the termination of System access for the offending Agency. All disputes concerning access shall be determined by a simple majority vote of the LARILJP Governance Committee.

IX. SIGN-OFF ON EXECUTION OF AGREEMENT

By executing this Agreement, each Agency acknowledges that it has received a copy of this Agreement, and will comply with its terms and conditions. This Memorandum of Agreement may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. A complete original will be kept on file with the Los Angeles City Clerk. For all other purposes, facsimile signatures are acceptable as originals.

Query-based Information Systems Approaches

This document describes three basic approaches for query-based information systems. These include a data warehouse, distributed query, and index. It includes a brief and high-level comparative analysis of each approach to inform executives and managers which approach might best meet their agency's needs.

Quick Overview

Information system type	What it involves...
Data Warehouse approach	This approach involves concentrating and managing a large amount of information contributed by participating agencies in a single repository.
Federated Queries approach	This approach simply routes each request to all available data sources and returns all the requested information.
Indexed approach	This approach typically contains a smaller set of key information provided by participating agencies with links to the originating system(s) to retrieve the complete set of information.

In essence, each approach—

- ◇ provides data from multiple data sources in a single query,
- ◇ requires a user interface, and
- ◇ requires some form of agreement among all participating stakeholders to confirm specific requirements.

Comparison

All the approaches achieve similar objectives; there are a few considerations that may affect an agency's decision on which approach best meets the needs of its users. The following comparison is a very brief assessment of the advantages and challenges of each approach. This is not to endorse one method over the other, but rather an attempt to make better informed decisions.

See the table on the next page for an at-a-glance comparison.

CENTRALIZED	<i>A centralized query application requires a repository large enough to accommodate a large set of data. Typically, these data are structured for efficient search and retrieval on a variety of search parameters.</i>
Advantages	<ul style="list-style-type: none"> ◇ <i>Analytics.</i> If you need to search for suspects with brown hair and eagle tattoos on the upper left arm, this is the best option. Centralized data warehouses support sophisticated logic for real-time associations, pattern recognition, and robust reporting capabilities. ◇ <i>Inexpensive to participate.</i> Typically, repositories accept “data-dumps” in a variety of methods that leverage the capabilities of the contributing system. This can occur in a number of ways (FTP, web service, etc.) and the frequency is usually flexible. ◇ <i>Reduced network traffic.</i> Queries to a central repository isolate end-user requests from the agencies that provide information. This prevents records management systems from being bogged down with constant external requests.
Challenges	<ul style="list-style-type: none"> ◇ <i>Data ownership and control.</i> Repositories require participating agencies to contribute information contained in their systems. Participating agencies have limited direction in <i>how</i> the information is managed in a repository. Strong governance and specific agreements can help mitigate this scenario, but the potential for inadvertent mistakes exist. ◇ <i>Information quality.</i> Due to the irregularity of reporting by the participating agencies, chances are a small amount of the repository contents are outdated or incomplete. This can manifest “false negative” search results. This does not imply the information is incorrect; it may not be complete. This is not applicable if all agencies update information in “real” real-time. ◇ <i>Limited scope.</i> Information can only be effectively used for investigations. While extremely powerful tools, repositories may not be the best option for integrating workflow or generating standard documentation like arrest reports, dispositions, etc.
DISTRIBUTED	<i>The distributed model consists of a basic application that simply sends requests to all available information sources. This approach may include a broker to route information among agency systems.</i>
Advantages	<ul style="list-style-type: none"> ◇ <i>Leverages existing information systems.</i> The distributed query approach will maximize information systems that are capable of responding to information requests. Typically, these include large, robust systems such as criminal history repositories, state court systems, or large agency records management systems. ◇ <i>Specificity.</i> This approach relies on structured requests and responses, providing accurate and detailed information.
Challenges	<ul style="list-style-type: none"> ◇ <i>Speed.</i> This model is simple and straightforward, but may require patience from the end user as the various information sources query results are compiled. General or vague queries will be slow and ineffective. ◇ <i>Requires significant bandwidth among stakeholders.</i> Distributed models send queries to all available information sources, which can strain network capabilities.
INDEXED	<i>The indexed approach also requires a repository, but on a smaller scale than a data warehouse. The data are also structured for rapid searching and response, and provide links, through brokering, to the point of origination, rather than containing the complete information set.</i>
Advantages	<ul style="list-style-type: none"> ◇ <i>Balance:</i> Indexing is a lightweight hybrid of the centralized repository and the distributed query. The repository provides quick responses from a variety of sources and provides additional information from the originating agency if requested. ◇ <i>Efficiency.</i> Index search results are typically very fast. A query for “which agencies have arrest records for Jane Doe” and then “give me the arrest records for Jane Doe” is a good example that highlights indexing capabilities. ◇ <i>Shared Administration.</i> The “pointer” information provided by participating agencies limits variations or misrepresentations of data, and allows for contributing agencies to retain control of subsequent, specific record requests.
Challenges	<ul style="list-style-type: none"> ◇ <i>Participant bandwidth.</i> Indexes may reduce the amount of traffic a participating agency receives, but the agency does need to accommodate the potential of responding to numerous requests, while meeting the day-to-day operations. This may require a replicated database, and may be cost-prohibitive to agencies. ◇ <i>Complex design.</i> The balanced approach can create difficulties, especially for smaller agencies, if the design becomes too complex, making implementation difficult.

APPENDIX B
Information Sharing Case Study: Los Angeles County, California