Law Enforcement Fusion Centers: Where Information, Technology and Policy Intersect

By ***Richard Johnston****, Chairman, Law Enforcement Advisory Board, LexisNexis Risk & Information Analytics Group*

Information drives society in many ways. Technological advances in the acquisition, analysis, and distribution of information over the past decade have fundamentally changed the way our society approaches life. We bank online, download videos, communicate instantly and continuously, travel using GPS systems, and "Google" everything. Vast libraries are available on demand.

From informal communications to critical decisions, we have become more dependent on large volumes of information acquired and processed in a timely manner. This data is then used to achieve specific objectives – whether making public safety decisions, designing medical protocols or constructing public policy.

Expectations for Law Enforcement

Law enforcement agencies in particular are expected to have and use the best technology available to protect citizens, respond to crises, conduct investigations, and prevent crime. Law enforcement also increasingly relies on new technology to identify potential terrorist threats. Automation through the use of advanced technology provides the capability to analyze large quantities of different types of information based on specific needs. Information sharing amongst law enforcement is progressing, both in the willingness and the ability, and yet, as capabilities enhance the collection, analysis, use, and sharing of information, the public also has a high expectation that this data will be protected, particularly their own personal information. This is an important and challenging issue for today's law enforcement executives.

Law enforcement agencies acquire various types of information that have rules about how, when, and by whom it can be used. The agency head must implement policies that ensure proper handling of these various types of information while not impeding access to and analysis of critical information. Most law enforcement leaders realize that limited resources require a high degree of efficiency in the approach to managing information. Today's most important focus is on merging these disparate pieces of information in a legal and useful way to ensure that information is used in the most effective manner. Public safety agencies are best served when they can obtain timely, accurate, and relevant information of different types in a way that provides an optimal amount of automated analysis.

Data Fusion Environments

Simply put, data fusion is bringing together large amounts of disparate information, analyzing that information, and using the results to make mission-critical decisions such as identifying and prioritizing targets, eliminating suspects, locating individuals who are evading apprehension, identifying hidden assets or associates, allocating resources, or simplifying complex elements of an investigation.

The concept of rules-based data fusion provides the best mechanism for law enforcement to meet its needs while addressing privacy concerns. Beginning in 2004, a concerted effort was placed on establishing guidelines for establishing and operating "fusion centers." Designated a priority by the National Governors Association, some 40 fusion centers are either in development or operating throughout the country. The critical issues surrounding fusion centers have been intensely examined by the Global Justice Information Sharing Initiative, a project of the Department of Justice and the Department of Homeland Security, through its Homeland Security Advisory Council. The resulting *Fusion Center Guidelines*, published in August 2006 by the Departments of Justice and Homeland Security, are an excellent resource for law enforcement decision-makers and provide a valuable framework for evaluating a number of critical issues involved in starting up a law enforcement fusion center.[1]

Increasingly, state and local jurisdictions are relying on these guidelines as the baseline requirements for fusion center development. In addition to covering the concept of data fusion, the guidelines cover 18 operational and policy areas – from governance and leveraging existing databases and networks, to interconnectivity and training.

Data Access, Information Sharing, and Privacy

Managing intelligence, incident reports, investigative reports, public records, open source documents, and other types of information from numerous agencies with independent missions in an environment of trust and security is a daunting challenge. The fusion concept offers an environment where these issues can be successfully managed. Critical mission-dependent decisions can be made on solid analysis of information from intelligence, investigative, and other agency files. Public records and open source information can augment this analysis, and within a fusion environment this can be facilitated with assurances of privacy protection if done with careful consideration and planning.

Among the recommendations made in the *Fusion Center Guidelines*, there are two that are perhaps the most critical for law enforcement to consider:

Leverage the databases, systems, and networks available via participating entities to maximize information.

- Obtain access to an array of databases and systems. At a minimum, consider obtaining access to driver's license information, motor vehicle registration data, location information, law enforcement, and criminal justice systems or networks and correctional data.
- Become a member of a regional or state secure law enforcement network, such as the Regional Information Sharing Systems® (RISS), Federal Bureau of Investigation's (FBI) Law Enforcement Online (LEO) system, DHS's Homeland Security Information Network (HSIN), or the FBI's Law Enforcement Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx).

Develop, publish, and adhere to a privacy and civil liberties policy.

- Develop, display, adhere to, and train personnel on the center's privacy policy.
- Consult the Fair Information Practices when developing a privacy policy.
- Ensure all other policies and internal controls are consistent with the center's privacy policy.
- Establish a process for tracking and handling privacy complaints or concerns.
- Develop rules on the use of privately held data systems information.
- Adhere to applicable state and federal constitutional and statutory privacy and civil liberties provisions.

While the prospect of implementing these two recommendations may present many challenges for law enforcement executives, there exists within the private sector a wealth of experience and expertise that can assist in both of these critical areas.

Role of Private Sector Partners

A close partnership between law enforcement and key private sector companies is a basic component of any successful fusion environment. The private sector has unique experience in identifying and solving problems by leveraging advanced technology and commercial best practices. Another crucial private sector role in fusion centers is providing the technology, analytical tools and public and open source data required to assist criminal intelligence analysts in their mission. The ability of private sector vendors to understand and respond to specific law enforcement requirements is the key to successfully applying these elements in the fusion center development process.

When the functionality of the center itself and the completion of the mission becomes a shared responsibility, the private sector's role takes on a new dimension. In the past, law enforcement may have been inclined to take on these challenges themselves, attempting to design, develop, and manage large, complex information collection, analysis, and sharing systems with all the attendant problems. Today, law enforcement agencies recognize the need for help in the form of highly credible, experienced private companies who can become working partners with law enforcement to meet information management needs.

As law enforcement officials work to implement the recommendations from the *Fusion Center Guidelines* that relate to data access, information sharing and privacy, there are numerous benefits to engaging the expertise of private sector businesses, including:

- **Data:** Electronic access to information acquired from public sources, reference data, and other open sources of information, integrated, and linked in a meaningful and relevant way, can be a powerful resource for fusion environments. This capacity to acquire, license, consolidate, and deliver information enables the private sector to provide fusion environments with a capability for accessing critical investigative information in near real-time that would normally take days for law enforcement officials to collect using traditional investigative methods.
- **Innovative Technology:** The private sector offers a variety of innovative technologies that can be leveraged within the fusion center environment for data fusion, collaboration, mapping and visual link analysis, as well as privacy-enhancing technologies. Fusion centers should optimize all available commercial technologies to help ensure their ability to protect individual's civil liberties and privacy interests, including use of such technologies as immutable audit trails to help ensure proper oversight and to deter the abuse of systems and sensitive information.
- **Policies and Compliance:** Working with private sector policy experts, law enforcement can benefit from understanding the relevant privacy policies that govern the use and sharing of investigative information and architect data fusion and information sharing systems in a manner that comports with these policies. These steps, perhaps more than any other part of the fusion center development process, are critical to the sustainability and long-term success of any fusion center, as they will help in fostering transparency and trust with the citizens the fusion center is designed to protect.
- **Information Security:** A private sector partner can also provide guidance and solutions for creating the high level of information security required in a fusion environment. When properly implemented in a comprehensive and layered fashion, security is a key enabler for privacy and policy compliance.

Conclusion

Data fusion is evolving as an advanced tool for law enforcement to address its mission, from public safety to counterterrorism. Large volumes of information, rapidly acquired and analyzed in an automated way according to the specific needs of the law enforcement mission are no longer a luxury, but rather a required tool to conduct criminal investigations, locate sexual predators and fugitives and protect critical infrastructures.

The success of fusion environments rests on careful consideration and implementation of many of the key recommendations of the *Fusion Center Guidelines* as well as identifying excellent private sector partners who can provide the technologies required and assist with the development of policy and procedures to ensure protection of the public's rights and privacy. ✪

About the Author: Mr. Johnston retired as director of the National White Collar Crime Center, where he served for 14 years. His prior experience includes serving as deputy director of the Louisville-Jefferson County, Kentucky Crime Commission and as director of Drug Enforcement Training at the Virginia Department of Criminal Justice Services. Mr. Johnston began his 34-year law enforcement career as an agent with the Bureau of Alcohol, Tobacco and Firearms, where he was instrumental in the development of the Bureau's training academy at the Federal Law Enforcement Training Center (FLETC).

Reference:

[1] *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era; US Department of Justice and US Department of Homeland Security, August, 2006.*

The *Fusion Center Guidelines* may be found at http://www.it.ojp.gov/topic.jsp?topic_id=209.