Introduction ....................................................................................................... 3
The Need to Share ............................................................................................ 4
An Overwhelming Availability of Information ............................................ 5
What Is Service-Oriented Architecture? ..................................................... 6
Next-Generation Justice Information Systems Versus Traditional Systems ................................................................................................................ 6
SOA and the Justice Community ..................................................................... 8
Modeling and Analysis .................................................................................. 11
  Technology from BlueForce ................................................................. 12
  How Exactly Does BlueInsight Work? .................................................... 13
Case Study: Louisiana Supreme Court ....................................................... 13
Conclusion ....................................................................................................... 14
INTRODUCTION

“Any member of the justice community can access the information they need to do their job, at the time they need it, in a form that is useful, regardless of the location of the data.”

This is the vision that the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC)—an advisory body to the U.S. attorney general, the assistant U.S. attorney general, and the U.S. Office of Justice Programs that was created to promote issues related to the exchange of justice information—described in the report “A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA).” Since that report, there have been a number of follow-up articles and practical initiatives that have attempted to further define and implement the principles and tenets that it champions.

Technology vendors and service providers alike have responded to this need to share information across jurisdictions and are offering solutions for real-time information access—regardless of the source or technology associated with that information. These solutions are developed around industry standards that enable disparate technologies to communicate using reusable, standards-based, network-accessible services. The infrastructure that supports this information sharing is called service-oriented architecture (SOA).

This white paper makes the case for the accelerated implementation of SOA, especially to support new, emerging technologies such as the modeling and analysis solutions that BlueForce LLC, a consulting firm, is developing for the justice community. Oracle, the leading innovator and provider of SOA technologies, and BlueForce have teamed up to help your agency realize the vision that the GAC describes above. Together, they are committed to the idea that technology alone cannot address information-sharing challenges. Rather, solving information-sharing problems requires a balance between people, process, and technology.
THE NEED TO SHARE

With the creation of the U.S. Department of Homeland Security (DHS) following 9/11, state and local law enforcement have seen significant funding of fusion centers, which are data hubs of intelligence gathering at the state, regional, and local levels for major metropolitan areas. The logic for this is simple: there are about 12,700 FBI agents, but there are almost 1 million state and local law enforcement officers. Given that terrorists perform conventional criminal acts either before or after major attacks, there is a greater chance that a terrorist will encounter one of these local officers rather than an FBI agent. Between 2001 and 2007, 58 regional, state, and local fusion centers have been partially or fully funded by the DHS. Those that were partially funded with federal monies have been supplementally financed by state and local agencies. The vast majority of these centralized intelligence centers are now operational.

Fusion centers are not solely concerned with vigilantly watching for terrorists. In fact, they are more likely tracking guns, drugs, repeat offenders, and gangs. It is estimated that there are more than 800,000 gang members in the United States involved in every type of crime, from drugs, prostitution, and human trafficking to arms dealing. And, like terrorist groups, they form cell-like organizations, spanning neighborhoods, cities, states, and even international boundaries. Groups like these—terrorist and criminal alike—are best handled through intelligence-led policing where the collection and dissemination of information, movement of evidence, and sharing of criminal records between systems work to locate all the pieces of a puzzle. Investigative case development supported by analytics supports putting the pieces together, while standards for data quality and privacy protect civil liberties and ensure the puzzle will successfully support apprehension and prosecution.

The ability to track cross-jurisdictional crimes will assist fusion centers across the country in solving crimes and potentially preventing the next terrorist attack. Although specific priorities can shift over time among terrorism, criminal networks like gangs, and emergency responses—ranging from child abduction to natural disasters—the basic need to share will remain the mandate for these fusion centers. These fusion centers are just the beginning of cross-jurisdictional information sharing efforts. As best practice techniques and supporting technology improvements are incubated at fusion centers, they will spread to other information sharing efforts between local, state, and federal jurisdictions.

---

AN OVERWHELMING AVAILABILITY OF INFORMATION

The amount of information available to the justice community today is overwhelming. In the past, finding information was the problem, but now the problem is filtering and processing huge and disparate data sets so that members of the justice community can fully exploit the available information. In fact, the problem is likely to get worse with the explosive growth of data and the number of repositories. The issue is further exacerbated by need-to-know access to the right data across multiple jurisdictions—a major issue for state and local fusion centers.²

During the tumultuous 1960s and early 1970s, the modern theory and practice of community policing was born out of studies challenging the assumptions that had grounded law enforcement policies for decades. Along with the rise of community policing, the justice community saw substantial growth in the demand for information technology (IT) with multiple uses. Unfortunately, as IT became more accessible and offered new capabilities, the applications available were still part of legacy, or stovepipe, systems based on data silos that were not easily upgraded or maintained.

During that time of great change for both police and the neighborhoods they served, there was a working group of young field police officers in Kansas City that recommended new initiatives based on lessons learned from landmark research in the “Kansas City Preventive Patrol Experiment.”³ One of the most significant discussions explored what would be possible in the future as IT grew in speed, capability, and capacity. The group thought of novel ways to empower those working in the law enforcement community to provide better service, if only IT could support access to information by officers when and where they needed it.

Recent police academy graduates are the ones most likely to be riding in patrol cars or walking a local beat. These younger members of the law enforcement community are of the internet-savvy generation and fully expect that the trends in internet services, such as mashups, Google, and Facebook, will be available to them as enterprise services that support their law enforcement efforts.

Remarkably, today is the future that has been long imagined; technology used by the latest recruits in their off-duty recreational and commercial activities is increasingly applicable to justice information systems. Most recently, the past six or seven years have seen a significant movement in the IT world that continues to accelerate and is rapidly gaining front-office use and acceptance, including in the justice community. The movement is to use technology built on service-oriented architecture (SOA).

WHAT IS SERVICE-ORIENTED ARCHITECTURE?

The use of SOA technologies is rapidly gathering momentum in both the commercial and public service sectors. The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) defines SOA as follows:

“SOA is an approach to the design and development of an information system. The assumption is that a system should be designed and developed around the basic components of the operational procedures or, in the language of the software literature, the business practices of an agency. These components are then combined into a loosely related larger structure that, in turn, can be combined into an even larger entity. It assumes, in other words, that the design of a system begins with a concept of the business practices of an enterprise (e.g., case-flow management, investigations, or trial preparation), which identifies the critical components (e.g., personal identification, sentencing document, or arrest report), which defines the parameters of stand-alone pieces of software (i.e., services). The effect is to permit the evolutionary development of a system.”

The key here is that the system is designed with the business in mind. Up until now, systems were put into place to serve particular organizations or lines of business, creating silos of information and gaps between these silos. Once an application or database is developed, it is very cumbersome to change. Business users are forced to conform to existing systems rather than have systems change with the business. In effect, a business process and the rules governing it are shaped by application logic and by existing permissions to associated data repositories. Such rigidity impedes innovation and hinders information sharing.

Oracle responds to this problem by offering solutions that put knowledge workers and their business processes in the foreground and create an agile infrastructure that supports productivity and aligns IT with the business. When referring to these technologies in the public sector, Oracle uses the term next-generation justice information system, which represents an organizational flow of data and application services between people, process, and technology.

NEXT-GENERATION JUSTICE INFORMATION SYSTEMS VERSUS TRADITIONAL SYSTEMS

Next-generation justice information systems will need to be agile, flexible, and fast. They must respond immediately to business needs, leverage existing infrastructure investments, and naturally adapt to future market demands and technology advances. In contrast, traditional systems are rigid and costly.

---

The following table highlights the differences between traditional and next-generation justice information systems:

<table>
<thead>
<tr>
<th>Next-Generation Justice Information Systems</th>
<th>Traditional Justice Information Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built for change and cross-jurisdictional use</td>
<td>Built for performance and siloed use</td>
</tr>
<tr>
<td>Composite applications</td>
<td>Application silos</td>
</tr>
<tr>
<td>Loosely coupled</td>
<td>Tightly coupled</td>
</tr>
<tr>
<td>Business process driven</td>
<td>Application function driven</td>
</tr>
<tr>
<td>Ingrained collaboration</td>
<td>Difficult collaboration</td>
</tr>
<tr>
<td>Real-time and batch electronic data sharing</td>
<td>Offline and paper-based data sharing</td>
</tr>
<tr>
<td>Heterogeneous horizontal integration</td>
<td>Homogeneous vertical integration</td>
</tr>
</tbody>
</table>

There are clear differences between current and next-generation systems.

Oracle helps agencies build next-generation justice information systems by focusing on five technologies:

- **Enterprise social computing.** Places the user and knowledge worker at the forefront through interactive, role-based secure portal and Web 2.0 technologies.

- **Business intelligence.** Provides analytical insight into trends and results presented by shared data sets and community expertise and observations.

- **Business process management.** Provides real-time visibility and control of the processes that run an agency through modeling, automating, and optimization.

- **Data integration and management services.** Provide the ability to query; redact; and extract, transform, and load data across jurisdictions. They also enable semantic matching, composite data set creation, and applied data quality approaches. These services can be used in real-time justice operations.

- **SOA infrastructure.** Transforms agency tasks into reusable, loosely coupled services and provides a secure, reliable infrastructure to support these services.
Next-generation justice information systems leverage five critical technologies to align business processes, information, and the people who use them.

These next-generation justice information systems provide the framework to implement a complete solution for information sharing in the justice community. Members of the community can aggregate information in real time from disparate sources, respond quickly through automated business processes, and get information out to people when they need it in a form they can use.

**SOA AND THE JUSTICE COMMUNITY**

Significant events such as 9/11 and Hurricane Katrina have highlighted critical limitations in information sharing within the justice community. Certainly, national security concerns drive law enforcement agencies to identify and track persons of interest. In times of natural disaster, it is crucial to be able to identify and manage an influx of first responders and relief workers, and to quickly re-establish disrupted infrastructure and operations. Programs such as AMBER Alert that expedite the safe recovery of missing persons—especially children—highlight the need to share information quickly and reliably at the national and regional levels.

Historically, law enforcement agencies, like other government agencies and large private corporations, have structured their IT assets into information silos according to agency-specific objectives. Interoperability and exchangeability were often an afterthought. However, in recent years the need to share information to address national security, disaster response, regional, and cross-agency concerns has driven enterprises toward SOA and data integration services improvements. SOA abstracts information away from its underlying data representation, application context, and location, and enables it to be made available to a broader user community. Network-based composite service applications make this information available, but also incorporate policy-driven governance to manage how, when, and with whom source data is shared.
In the data silo model, to gather information, authorized personnel must search different systems (such as the National Crime Information Center database, state departments of motor vehicles, state criminal records, and social welfare systems) on different networks with different login credentials and data schemata. They must then manually assimilate data from these various sources—often after heated negotiations with data stewards over when, how, and to what extent data is to be fused with other, shared data sets. This method is very inefficient, with the potential for one-off governance, overlooked linkages, and cumbersome point-to-point access to retrieve data. For example, in fusion centers the security protocols between federal intelligence sources at the DHS and FBI often become roadblocks to sharing information with the state and local fusion centers.5

One early effort to automate the retrieval and assimilation of this data has been the National Law Enforcement Telecommunications System (NLETS). This system is a frame relay–based message-switching system that links state, local, tribal, federal, and justice information systems for data exchange. The NLETS provides the user with a portal interface as a common point for accessing multiple systems. It switch-forwards queries to the appropriate systems and returns the data to the inquiring end-user. However, the issue of mapping data in potentially disparate formats has remained a challenge. The NLETS provides some ability to normalize data returned from queries, but a point-to-point mapping at the user access portal was considered the only viable option for providing a uniform query interface.

This issue of resolving data representations led the U.S. Department of Justice (DOJ) and the state departments of justice to develop the Global Justice XML Data Model (Global JXDM6) under the auspices of the Office of Justice Programs and GAC. The Global JXDM model reduced point-to-point data mapping problems to a canonical data exchange. Global JXDM set the stage for broader data-exchange standards through the National Information Exchange Model (NIEM)—a model developed through a partnership between the DOJ and DHS with the mission to design, develop, support, and disseminate enterprise-wide interoperability standards. Under NIEM, Global JXDM, with its data model, data dictionary, and XML schema, is just one of several data contexts, each with its own defined namespace, common data descriptions, and data-sharing guidelines.

Still, resolving data interoperability issues is just part of the complex problem of effective information sharing. In addition to the NLETS, several other systems have been developed to leverage Global JXDM and NIEM to build Web-based services to retrieve legal information: the Homeland Security Information Network, Regional Information Sharing System, and Law Enforcement Online. Unfortunately, all these systems—like the original silos—were built for agency

purposes, with information sharing capabilities a mere afterthought. Because agencies have yet to resolve access issues and usage inconsistencies across these systems, a truly federated shared-information environment has not yet been achieved.

The next large-scale effort to share law enforcement information and address the limitations of previous systems is the DOJ’s Law Enforcement National Data Exchange (N-DEx) program. N-DEx will provide a mechanism for users to upload and share information, and add governance so that any security protection that information providers elect to apply can be maintained. One key point here is that information providers can maintain ownership of their information and control how it is shared with the broader community. As N-DEx begins to come online, expect to see other SOA attributes.

Even as large-scale systems leverage SOA principles to facilitate service-based capabilities, there are similar frameworks being used on a smaller scale within the scope of local and state agencies. The GAC promotes SOA as the framework for justice community information sharing. Many state fusion centers, as well as court systems and other in-state agencies, find SOA a practical solution to a complex problem. This is the beauty of SOA: in its distributed software model, small pieces of application functionality are published, consumed, and combined with other applications, over a network and on demand. The data’s owner retains control over it, but, consistent with the GAC’s vision, “any member of the justice community can access the information they need to do their job, at the time they need it and in a form that is useful, regardless of the location of the data.” SOA reuse of component services promotes cost efficiency and sustainability. Likewise, the standards-based component nature of SOA supports extensibility and interoperability with other external systems.

It’s not likely that there will be a single, all-encompassing information sharing system for the entire law-enforcement community. An individual organization’s needs, policies, and processes (not to mention their desire to maintain control over their local data) are too diverse to expect that a single system could meet all needs. However, SOA-based systems do provide the foundation for a federation of systems to provide critical capabilities to law enforcement personnel.

The major differences between the next-generation justice information system’s use of SOA and the expectations borne out in the previously mentioned report “A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)” are around how SOA will differ from initial expectations. First, next-generation justice information systems will be driven by operational justice processes such as criminal investigations, terrorist entity extractions, AMBER Alerts, natural disaster responses, and other domain-specific business processes. These processes will increasingly dictate which applications—both legacy and new—are used and how they will be extended. SOA will provide the glue and flexibility to reuse these applications based on the domain-specific business process, changing the applications instead of the processes.
Second, with the next-generation justice information system, there will be far more information shared in dynamically assembled, collaborative teams, based on need-to-know (as opposed to who-you-know) access to the appropriate level of information. This access will be tightly controlled with fine-grained redaction of requested data record elements at the source location, transformed in accordance with Global JXDM or NIEM within the SOA layer, typically at a state or local fusion center or an equivalent shared data center. Use of this next-generation system will be driven by the cross-jurisdictional operational process implemented within the SOA platform through a combination of business rules. These rules will be based on predefined cross-jurisdictional policies and implemented in the SOA orchestration layer. They will provide high levels of information assurance and alleviate many of the governance hurdles faced by data stewards.

MODELING AND ANALYSIS

Routine application of modeling and analysis technologies for prediction and planning are still relatively new in the justice community. Although they have been topics of research, development, and application for the commercial and U.S. military domains for some time, they have only recently offered advantages for law enforcement as well. Ongoing implementation of SOA initiatives in the justice community is causing an increased availability of large data sets from which powerful predictive and planning models can be built. This synergy is destined to make modeling and analysis technologies for predicting and planning more and more affordable for justice community agencies everywhere.

Modeling involves the crafting of computer simulations that mirror the characteristics of real networks. In the language of military practitioners:

“A Human Network is a formal or informal social structure made of nodes (individuals or organizations) that are tied by one or more specific types of interdependency, such as values, ideology, financial exchange, kinship, common enemies, conflicts, or trade.”

But today’s ranks of military practitioners include recent graduates from military academies and Reserve Officers’ Training Corps programs around the country who are proficient and reliant upon social computing networks. They are looking to leverage SOA and its ability to transform data integration and composite application services into their secure information collaboration systems.

An article in GCN magazine explored how the defense and intelligence community views the risks of adopting new information sharing technology and Web 2.0 applications such as social networking mashups and wikis. To maintain information security in the new environment, military leaders are building safeguards into enterprise architecture—but nonetheless implementing them.

---

“I think the answer to the security issues is in the platform,” Defense Information Systems Agency CIO John Garing said at an AFCEA Defense 2.0 conference. “If we don’t secure the platforms, the young people will run right past us.”

The specific systems and business needs of the military intelligence community are certainly different from those of the law enforcement intelligence community. However, the example highlights the similarities between the two groups. Namely, both groups grapple with how to use technology with each new generation of officers, agents, and analysts; how technological evolution and its adoption affects new business areas; and how to implement SOA to meet the needs of the intelligence community.

Technology from BlueForce

BlueForce advocates the development of modeling and analysis technologies for prediction and planning as a prime area where the justice community can be more effective in accomplishing its difficult mission. These technologies continue to be applied in the military domain to gain an edge in combating terrorist cells. For example, one development concerns the frequent experience that soldiers have with improvised explosive devices in Iraq and Afghanistan. Modeling the groups responsible for building and deploying these devices is expected to yield benefits by providing information that helps to predict the effects of various interventions to deter such building and deployment. U.S. military strategists routinely use modeling and analysis technologies to aid in planning processes. These technologies will continue to grow in reliability and efficiency as models in a variety of domains are tested and improved iteratively across domains.

BlueForce, in partnership with the New England Complex Systems Institute, is developing a suite of network-dependency and consequence-analysis technologies under the trade name BlueInsight. These technologies will empower justice community practitioners—including police officers, planners, and executives—to be more effective in identifying, exploiting, targeting, and disrupting criminal organizations. These technologies will be equally valuable when developing strategies to respond to emergencies such as hurricanes.

BlueInsight will make it possible to represent networks of people, places, objects, and concepts using computer technology and display them on a monitor for manipulation and testing.

As SOA facilitates access to more information, concerns in the justice community become less about gaining the ability to access information and more about being able to use it more effectively. This is where the ability to model real events and
conditions on the ground is so important. Modeling and analysis technologies are tools to help members of the justice community think, relieving them of the mundane tasks of assembling data and leaving them free to give their attention to real analysis.

**How Exactly Does BlueInsight Work?**

SOA and other justice community standards and protocols comprise the framework that facilitates data collection for the BlueInsight Suite. Data from many disparate sources is processed, mapped, and analyzed to provide information to populate a model of nodes that represent real people, places, objects, and concepts. Distinguishing key linkages between these nodes and quantifying their dependencies on each other adds context to the data. The BlueInsight Suite uses a proprietary algorithm to compute the overall effects of alterations anywhere in the model. The information revealed in the model will be useful when developing possible courses of action and matching goals to resources. Users of this technology will be able to compute the consequences of various action options inside the model. The results of these computations will be useful for predicting likely results of such actions if they were applied to the real world. As the model is perpetually updated with feedback, it is expected to gain accuracy as a predictive tool. The BlueInsight Suite can build plans and produce analytic reports and schedules that take into account the predictions the model makes possible.

BlueInsight merges cutting-edge technologies with specialized research into semantic-level integration. It represents the convergence of advances in the areas of database integration, Web standards, and knowledge representation all leveraging Oracle Fusion Middleware as its SOA platform.

In summary, SOA makes access to vast data sources easier and more universally affordable. The BlueInsight Suite is one example of an emerging technology that takes advantage of the availability of the large data sets that SOA enables.

**CASE STUDY: LOUISIANA SUPREME COURT**

The Louisiana Supreme Court is the state’s highest court, managing child and family, drug, and other specialized state cases as well as typical court cases. In total it receives and processes nearly 3,000 cases per year.

In addition to its day-to-day court proceedings and associated record keeping, the Louisiana Supreme Court receives 300 to 500 Certificate of Good Standing requests per month. Up until recently, these were all handled manually, then copied and distributed to members of the review team. However, the court adopted an SOA approach to automate these processes and make the documents available via digital media using the Oracle Business Process Management and Oracle WebCenter Suite Interaction tools. This significantly increased employee efficiency through robust collaboration and search tools, and also increased visibility into and
optimized case management. As a result, the Louisiana Supreme Court expects productivity to increase by 50 percent.

“We cannot talk about the Louisiana Supreme Court without talking about Hurricane Katrina,” explains Peter Haas, the court’s director of technology. “During and after Katrina, our Web-based portal helped us in many ways.” In the midst of the hurricane, all operations, hardware, and everything that supported the Court had to be relocated. In addition, says Haas, “people could not get back to where they lived.” The portal provided a single source of entry, which was a security assurance. “It didn’t matter if one was using a different system, customized or off-the-shelf software. One could just log in and work,” says Haas. “Though many people were displaced, we could still communicate wherever we were.”

It is interesting to note that the court’s existing business process management, user interaction, and information sharing technologies from Oracle were not part of a prior plan for continuity of operations. However, after the devastation of Hurricane Katrina completely disrupted normal operation, court employees realized they already had the tools in place to quickly re-establish business processes; to allow displaced employees, lawyers, and the public to interact with the court remotely; and to return court operations to some sense of normalcy. The agility of this technology was extremely valuable in returning the court’s functions to the citizens of Louisiana.

CONCLUSION

SOA and the next-generation justice information system do not have to be implemented all at once. Information sharing within the justice community can be approached incrementally and from different angles. The ultimate goal will be to enable faster response times within your agency and to citizens and police officers on the street.

Oracle and BlueForce bring together the necessary law enforcement community expertise, industry-leading technology, and consulting resources to meet your information sharing needs. Oracle and BlueForce are ready to take your initiative to the next level. They will work with you to identify which sources are most important to integrate, where you might have information gaps, which manual processes could benefit from automation, the importance of governance and federation to information sharing, and other important aspects of service-enabled information access.