

Blueprints for Change: Criminal Justice Policy Issues in Virginia

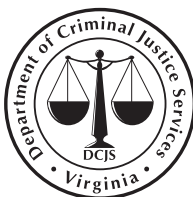



**DATA MINING AND
REGIONAL NETWORKS AS
AN INVESTIGATIVE TOOL:
ADMINISTRATIVE AND POLICY
CONSIDERATIONS**



Virginia Department of Criminal Justice Services
www.dcjs.virginia.gov

May 9-10, 2007
Staunton, Virginia



The Department of Criminal Justice Services (DCJS) is the state criminal justice planning agency in Virginia and is responsible for administering state and federal funds dedicated to improving state and local criminal justice practices, preventing crime and delinquency, and ensuring services to crime victims.

In its role as a planning agency, the Department convened six policy sessions over a two day period in May, 2007. The facilitated sessions explored six different leading edge criminal justice issues, chosen by the Department. Each three-hour session brought together a multidisciplinary group of executive-level participants who were selected because of their knowledge of the issue and their ability to advance the discussion of public policy related to the issue.

The discussions in these sessions, and the recommendations that emerged, are recorded in these policy papers.

In publishing these papers, DCJS hopes that they will stimulate further discussions by state and local decision makers and will provide useful guidance for making substantive statutory change where necessary, as well as for decisions on funding, and policy and program development.

The 2007 Blueprints for Change: Criminal Justice Policy Issues in Virginia documents are:

Canine Training and Law Enforcement

Data Mining and Regional Networks as an Investigative Tool: Administrative and Policy Considerations

Evidence-Based Practices in Community Corrections

Sexual Assault Policies in Virginia Law Enforcement Agencies

Using Technology to Guard Against Bias in Policing

Virginia's Response to the JJDP Act's Sight & Sound Separation Requirement

**For additional information on these documents, please visit the
Department of Criminal Justice Services website at: www.dcjs.virginia.gov**

Data Mining and Regional Networks as an Investigative Tool: Administrative and Policy Considerations



The August 2006 *Blueprints for Change* policy meeting, convened by the Department of Criminal Justice Services, recognized Virginia has been developing regional crime information sharing networks for more than a decade. These networks have allowed criminal justice agencies to share information about crimes, suspects and leads in criminal investigations. Traditional methods, such as mailing and faxing papers or telephoning neighboring agencies, have become obsolete in the age of instant access and information driven decision-making. But there can be a downside – too much information. Investigators sometimes find themselves in the position of being unable to sort, prioritize or even develop relationships among data because the volume of information makes it nearly impossible to identify the important items. Thus, criminals escape detection and apprehension as the result of critical data being lost in the immense number of reports and documents available.

One strategy for extracting meaning from large amounts of investigative information is the use of “data mining” applications. Data mining systematically searches information to identify relationships and patterns. Although data mining has been used effectively in private industry for a number of years, law enforcement has trailed in the application of this technology. As an interesting comparison, data mining techniques in the commercial environment have allowed retailers to know more about purchasing habits than what the police know about criminal suspects.

To explore the use of data mining within law enforcement and discuss associated policy issues, the May 2007 *Blueprints for Change* meeting brought together representatives from various localities that currently use regional information sharing networks and data mining software. Representatives from agencies considering the implementation of data mining systems were also present.

Panel participants included police chiefs, sheriffs, Virginia State Police officials, information technology directors, municipal officials, and staff from the Department of Criminal Justice Services’ Technical Services Unit. Participants shared their experiences from involvement in the development of regional information sharing networks operating in Virginia.

The regional network environment in Virginia is different from other states. Regional networks in most states have been developed for metropolitan areas, with no plan for integrating the various networks. Virginia’s nine regional information sharing networks serve both metropolitan and rural areas and each will be included in a proposed statewide network of regional information systems. *Blueprints* participants endorsed the goal of including all of Virginia’s local law enforcement agencies in the development of future information sharing networks.

Within Virginia, the Mountain Empire Criminal Justice Information Network (MECJIN), the Rappahannock Regional Crime Information Network (RRN) and the Hampton Roads Law Enforcement Information Exchange (LInX) use sophisticated data mining software. MECJIN and RRN use a Memex data mining product while LInX uses software developed for the U.S. Naval Criminal Investigative Service. Regional networks currently under development to serve the Danville, Roanoke and Northern Virginia areas will also include data mining systems.

Data Mining in Use – Rappahannock Regional Crime Information Network

The Rappahannock Regional Crime Information Network is an example of how criminal justice agencies in Virginia are using data mining. The RRN links the Fredericksburg Police Department and the Sheriff's Offices in King George, Spotsylvania and Stafford counties. The RNN provides for the compilation of information from criminal activity reports, Computer-Aided Dispatch (CAD) system data, Incident-Based Report (IBR) data and other information sources from the criminal justice agencies that participate in the network. RNN users use data mining software to search compiled information and discover relationships. Because of the size and disparity of the data compilations being queried, these relationships might not be easily detected using traditional data analysis techniques or manual records searches.

Data mining software consists of sophisticated search programs, advanced statistical techniques and innovative graphics features. Search programs used in data mining software provide users with abilities to make queries that use varied search criteria and repeatedly redefine those criteria to make searches as useful as possible. By using data mining software, investigators can initiate database searches and link analyses that extract information describing relationships between persons, events and other aspects of criminal activities. Data mining systems provide users with graphic displays that make it easier to see the detected relationships or patterns.

A typical law enforcement data mining application might attempt to identify a suspect when the only available information is a crime report and a vehicle description. An investigator could initiate a query of a regional network database to obtain information that would identify a suspect. Data mining software would then search information compiled by all agencies participating in the network. The vehicle description contained in the crime report submitted by one agency might match an entry in a field interview report submitted by a different agency. The field interview report might indicate the vehicle was seen a short distance from the crime scene at a time close to the time of the crime and that its driver had been questioned and provided a name and address. Data mining software could then be used to determine the involvement of the now-identified suspect in other crimes. Without the advantage of data mining software, information from the crime report and the field interview information might never have been linked.

The 2002 "D.C. sniper" investigation illustrates the difficulty in searching massive amounts of information available to law enforcement agencies. During that investigation, multiple law enforcement agencies were compiling information, resulting in the availability of a large amount of data in various systems. Review of the investigation revealed that information on the vehicle used by the snipers had been previously reported by law enforcement agencies, but the volume of data and its storage in disparate systems precluded timely searches. Data mining addresses this problem.



POLICY/RESEARCH QUESTIONS

The panel examined several issues that must be considered when using data mining technologies:

1. How can law enforcement agencies balance the need to review broad sets of information during criminal investigations with the privacy concerns of citizens?
2. What administrative and logistical issues must be addressed to effectively and efficiently manage the creation and maintenance of law enforcement information sharing agreements?
3. What strategies can be applied to access the funding and technical expertise needed for the development and implementation of data mining systems?
4. How can relationships between state and local law enforcement agencies be managed to enhance information sharing initiatives?



DISCUSSION

Privacy

Any use of data mining as an investigative tool by law enforcement agencies will raise privacy concerns from the public. To that end, information sharing and data mining technology is advancing more rapidly than the regulations or professional standards that control their usage. Using regional networks to access broad sets of public information for the purpose of exposing criminal activity or involvement will likely raise fears of misuse of information gained through this technology application.

Although privacy is a concern commonly cited, most of the panel members stated they have seen very little indication of public concern about their use of data mining technology. Interestingly, panel members had opposing views on why this is the case. One view is the public is simply unaware these data mining capabilities exist or is unaware local law enforcement agencies are using them. The other view is the public assumes law enforcement agencies already have this capability, use it frequently and it is considered so routine they are not concerned about it. One panel member noted the public may have an exaggerated view of what these systems are capable of doing. This was attributed to its depiction on television and within movies. It was also suggested there might be a crime prevention benefit to allowing people to think these systems can do more than they really can.

Regardless of which view is correct, the panel agreed that the public's concern about privacy needs to be considered. This raised the question of whether state and local law enforcement agencies should proactively consider how they respond if the public or media approach them with questions about what they are doing with these technologies and why. Should there be proactive public education to address the privacy concerns rather than responding to inquiries as they occur?

One way of addressing these concerns is to recognize that there are regulations and guidelines in place to limit how these systems are used. Agencies are not free to collect, maintain and analyze any type of information about any citizen. The primary regulation on these activities is Part 28 of the Code of Federal Regulations – 28 CFR. (28 CFR is available at www.iir.com/28cfr/guideline.htm. Assistance with applying its provisions to information compilation and transmittal is available from DCJS' Technical Services Unit.) The regulations were written to protect the privacy rights of individuals and to encourage the expeditious exchange of criminal intelligence information between law enforcement agencies. The regulations allow criminal intelligence information to be put into a criminal intelligence sharing system only if it is relevant to the identification of and the criminal activity engaged in by an individual or organization reasonably suspected of involvement in criminal activity and meets criminal intelligence system submission criteria.

The regulations that govern the basic requirements for operation of a criminal intelligence system include:

- Information submission or collection
- Secure storage
- Inquiry and search capability
- Controlled dissemination
- Purge and review process

It was noted that most of the commercial data mining packages developed for law enforcement have the capability to provide detailed audit trails of all queries of the system and can maintain and purge data records for 28 CFR compliance.

Another method for meeting privacy concerns is requiring the agency to restrict access of information to only those who need it. Different types and levels of data can be accessed based on selectable criteria. For example, detectives may be given access to certain data that is not accessible to patrol officers.

Administration

Because data mining through a network typically involves providing multiple agencies access to each other's systems, administrative issues must be considered. The following issues were discussed by participants:

Which agency 'owns' the data mining equipment and software?

All of Virginia's regional networks are operated using a shared costs policy. Data mining system costs are shared among participating agencies and those costs are based on a formula that usually provides for charges in accordance with the amount of system usage. Regardless of the costing formula used, obtaining funds to procure and implement data mining technology presents a challenge, especially for less affluent rural localities. While data mining software offers important benefits to law enforcement users, it is expensive. All of Virginia's networks that offer data mining rely heavily on grants from DCJS for data mining software procurement and most receive substantial technical assistance from the agency's Technical Services Unit.

Who provides system support services?

The successful use of data mining software requires dependable support services. While the most popular data mining products are "user friendly," data mining packages are complex. Since the software is also relatively new, its developers are releasing frequent revisions and enhancements. These two factors make adequate support essential. In Virginia, the regional networks that use data mining software rely heavily on information technology personnel for system support. The Rappahannock Regional Network has a full-time network administrator who is responsible for providing support services, including user training. The Mountain Empire Network is currently establishing such a position.

What data will each agency supply to the system hub?

In Virginia, the type of information submitted by participating agencies varies among networks. Agencies participating in the Mountain Empire Criminal Justice Information Network submit all of their computer-aided dispatch, records management system and jail management system data. Other networks only provide for the compilation of selected records management system information. Panel members agreed that the type of data compiled by a network is not as important as the need to determine, prior to completion of network development, information submission requirements that are acceptable to all network member agencies.

How is the quality of the data available for data mining maintained?

This is important because data mining is sensitive to subtle differences in data quality. Poor quality data that might go unnoticed amongst huge amounts of other data could be critical in data mining, where every piece of data can be examined and potentially acted upon. In Virginia's networks, each participating agency owns its own data, since it has the most interest in being sure it is correct. This insures that those who best know and understand the data can control its quality before it is made accessible to other users.

How timely is the data?

In some cases, data that is weeks or months old can be valuable. But in other cases, data mining depends on access to current information to identify emerging trends. This is especially relevant when data mining is used to make predictions about future criminal activity. This concept of "predictive analysis" is becoming increasingly important to law enforcement agencies as they strive to manage their limited resources in the fight against crime. The timely updating of criminal investigations is also significant, as it may

prevent unintended concurrent investigative efforts and contribute to the more effective use of investigative resources. Additionally, routine information on such issues as warrants and expungements must be kept current to maximize the potential of the systems.

Access to Funding and Technical Expertise

The discussion of the cost and support requirements for data mining systems prompted one panel member to suggest that DCJS develop an “inventory” of information systems being used by public safety agencies in Virginia. The impetus for this suggestion was the panel member’s concern that, while some Virginia localities are moving ahead with implementation of new technologies, other localities, particularly rural areas, are still using older and less sophisticated systems. Several panel members agreed that, for some less affluent Virginia localities, the development of regional networks and the implementation of data mining systems represent substantial budgetary challenges. Nonetheless, panel members concurred that the disparity between information systems needs to be reduced. An on-line inventory of information systems technology being used by Virginia public safety agencies would provide users with a valuable resource. The inventory could guide agencies toward the procurement and implementation of more advanced and compatible systems. Panel members suggested that DCJS develop and maintain the proposed inventory and make it available on the agency’s web site.

Panel members stressed that efforts aimed at reducing the disparity between Virginia’s law enforcement information management systems should not detract from DCJS’ focus on continuing the development of regional information sharing networks. The panel endorsed the concept of developing a statewide network of regional networks that will include all of Virginia’s local law enforcement agencies. Additionally, the panel agreed that regional network development projects should maintain a priority status for the receipt of grant funds and technical assistance.

Relationship Between State Efforts and Local Efforts

Any efforts to develop data mining capabilities should be done with an awareness of emerging state and federal efforts, because these projects often set standards and procedures with which local systems must interface. The discussion on these issues was led by a representative from the Virginia State Police (VSP) Fusion Center who is a member of the Commonwealth Intelligence Working Group.

Most of the panel’s discussion centered on how local systems and regional networks would interact with the state’s new intelligence information sharing system, the Virginia Intelligence Management System (VIMS). VIMS is being designed to replace VSP’s Tactical Intelligence Processing System (TIPS), which did not provide the functionality that will be available with VIMS. While it is still early in the VIMS development process, preliminary planning indicates the system will provide its users with a powerful resource for sharing and analyzing intelligence data.

VIMS has been developed as an effort to address the need for law enforcement to share intelligence information statewide and improve the quality of intelligence data. VIMS is being designed to provide a clearinghouse for intelligence information compiled by Virginia’s law enforcement agencies. Selected information compiled by records management systems used by local law enforcement agencies will be submitted to VIMS. Agencies that participate in regional information sharing networks will use their regional network hub as a “portal” to submit information to VIMS. After information has been submitted to VIMS, State Police Fusion Center staff will determine if it qualifies as intelligence information. If so, VIMS will maintain the information and make it available to system users. VIMS-maintained information will be available for use by, or exchange with, users throughout Virginia. VIMS implementation will also result in improved quality of intelligence information. The Fusion Center will apply data quality standards when reviewing

all submitted information and only data that meets those standards will be accepted. This will establish a consistent standard for intelligence information instead of the continued application of criteria that differ from one agency to another.

VIMS will be available to all local law enforcement agencies, providing they are 28 CFR compliant, have the appropriate equipment and a trained staff analyst, and a VIMS usage agreement with VSP. While VIMS will be operated by VSP, the system will be used by investigators and analysts in local law enforcement agencies and federal agencies, as well as by VSP staff. VSP and DCJS are working together on making VIMS training available at Virginia's regional criminal justice academies.

VIMS is being designed to:

- Be 28 CFR compliant
- Provide query capability to all local records management systems
- Contain geographically-coded data
- Provide different levels of data access
- Provide information supporting both anti-crime and anti-terrorism activities

Several panel members suggested that VSP should include local law enforcement agencies in the VIMS planning process. Panel members recommended that local agencies be involved in the development of data standards for VIMS and voiced the concern that VSP will require use of VIMS, but not provide the resources needed for participation. VSP staff responded that local law enforcement agencies and DCJS are represented on the VIMS Implementation Committee, which is advising VSP on development and implementation, and expressed their interest in having meetings with Virginia's sheriffs and police chiefs to obtain their views on VIMS and the capabilities it should offer.



CONCLUSIONS AND RECOMMENDATIONS

Panel members agreed that VIMS and data mining technologies are a valuable resource for the sharing of intelligence information. However, the following conclusions and recommendations were noted:

1. More discussions between VSP and representatives of local law enforcement should be initiated before the development of VIMS is complete.
2. The development and dissemination of model policies for intelligence data compilation would be useful for all law enforcement agencies. These model policies should complement VSP policies and data collection protocol for future information sharing compatibility.
3. DCJS should research and make available a resource document of public safety technologies that are available to local agencies.
4. DCJS should develop a resource document of information systems being used by Virginia's local public safety agencies to enhance regional network planning and promote collaboration among agencies.



PARTICIPANTS

Mr. Gregory Call, *Director of Information & Tech., Rappahannock Regional Jail, Stafford, Virginia*

Chief Richard Clark, Jr., *Galax Police Department, Galax, Virginia*

Chief A.L. “Joe” Gaskins, *Roanoke City Police Department, Roanoke, Virginia*

The Honorable Charles E. Jett, *Sheriff, Stafford County, Stafford, Virginia*

The Honorable E. Stuart Kitchen, Jr., *Sheriff, Sussex County, Sussex, Virginia*

Lieutenant Steve Lambert, *(Workshop Presenter), Virginia State Police, Richmond, Virginia*

Chief J.R. Lavinder, *Roanoke County Police Department, Roanoke, Virginia*

Chief William A. Puckett, *Richlands Police Department, Richlands, Virginia*

Captain Len Terry, *Virginia State Police, Richmond, Virginia*

Ms. Kimberly Vanhoy, *Smyth County Information Systems, Marion, Virginia*

The Honorable Ryant L. Washington, *Sheriff, Fluvanna County, Palmyra, Virginia*

DCJS Staff

Ms. Eileen Guertler

Mr. Butch Johnstone

Mr. Joe Marshall

Mr. Jim McDonough

Mr. Chuck Ruble

Mr. Ben Wood *(Workshop Facilitator)*



Virginia Department of Criminal Justice Services
202 North Ninth Street, Richmond, VA 23229

www.dcjs.virginia.gov