New York City Criminal Justice DataShare

Technical Strategy Subcommittee

Final Report
June 2003

Acknowledgment

Recognition is due to all of the members of the DataShare Technical Strategy Subcommittee for the hard work and zeal that they brought to preparing this report. Together, the Subcommittee members dedicated dozens of hours to researching and learning about new integration technologies, discussing business requirements and analyzing what solutions would best serve the New York City criminal justice system. In addition to their demanding jobs at their respective agencies, members dedicated many, many hours to making this project a success. Several Subcommittee members went above the call of duty: Kael Goodman, William Power and Robert Schlesinger deserve special thanks for their dedication and leadership over the past five months. They led the Subcommittee and were the primary drafters of this report.

Bob Plikaytis and the DoITT team also deserve recognition for their important contributions to the Subcommittee and their ongoing efforts in maintaining the DataShare system. They have been invaluable partners.

Table of Contents

Executive Summary

Introduction & Methodology

This is the final report of the Technical Strategy Subcommittee[1] ("Subcommittee") of the New York City Criminal Justice DataShare Executive Council ("Executive Council"). This Subcommittee was established by the Executive Council to evaluate the existing DataShare system in light of technical advancements made over the eight years since the system was designed, and to determine if these technical advancements could be called upon to: (1) improve criminal justice outcomes by providing criminal justice practitioners with more information in a timely and usable fashion; (2) enhance the inter-agency business practices of NYC criminal justice agencies; and (3) enable criminal justice agencies to do more with less.

Over five months, the Subcommittee: (1) studied functional requirements set forth by the Executive Council and identified additional desired functionality; (2) explored integration successes from other jurisdictions; (3) assessed the DataShare system and other DoITT-maintained technologies used by criminal justice agencies to communicate; (4) educated participating IT staff about state-of-the-art data integration technologies; (5) discussed specific implementation tools and strategies; and (6) generated conclusions about the feasibility of replacing the existing DataShare system.

Conclusions

Based on this research, the Subcommittee has concluded that the New York City criminal justice system can leverage technology to improve upon the gains made since the inception of Datashare in 1995. Upgrading this infrastructure would enable us to do things like:

- ✓ Distribute appropriate NYPD information throughout the criminal justice system;
- ✓ Provide comprehensive arrest & complainant information in a timely fashion to district attorneys and other criminal justice players;
- ✓ Automate the preparation of Department of Probation Pre-Sentence Investigation reports ("PSIs") by extracting data from existing sources;
- ✓ Provide timely notifications of changes in inmate status from DOC to detectives and prosecutors.

The Subcommittee recommends that the existing DataShare system be replaced with a central hub that would provide secure, flexible data communications through a messaging infrastructure. The central hub would control security. As with the existing DataShare system, individual agencies would determine who among the criminal justice system users would have access to their data. Different users would have different privileges that would govern their access to data.

---

[1] See Appendix D for a list of members.

Functionality

The Subcommittee has concluded that the functional improvements identified by the Executive Council could be achieved using readily available technology. Production requirements, where one agency uses data from another to support day-to-day operations, could be expanded. This would accommodate the increasing complexity and depth of data being captured using information technology at all of the agencies. Automatic updates would be sent to individual agencies if data were needed to conduct business (push), or made available to them upon request (pull). Staff at different agencies -- a detective at the police department, an assistant district attorney or a probation officer, for example -- could subscribe to automatic notifications or warnings when a qualifying event (such as a second arrest or a defendant's release from jail) was recorded in another agency's system. Information could be moved either as a document (file sharing) or as data (data sharing).

The central hub would be directly accessible by agency case management systems or by end-users. Agency case management systems would be provided with the capability to "speak" to the hub's middleware software. For instance, when a user hits a "Jail" button for a particular defendant within his/her agency's internal case management system, that system would make a "behind-the-scenes" request for DOC's jail status. The agency's data would be formatted back to the user within the already-familiar program. Such access would provide a completely seamless integration with agency systems, and would, in a sense, make the hub invisible to the user.

In other situations, users would access this system via a user-friendly browser-based front-end. This "public safety portal" would be a significant improvement in usability over the current tools that are in place. District attorneys, police officers and probation officers would no longer operate without valuable information because they do not know the key strokes to access other agencies' "green screen systems" or do not have access or individual passwords to each of the criminal justice applications available to them. Users would have a tool that is as easy to use as the internet. Agency technology departments would have the ability to provide their users with access to information in the way that makes the most sense based on business needs and resources.

Best Practices

These conclusions are further supported by the finding that numerous jurisdictions have taken advantage of technological advancements over the last 5 years and have achieved great results: New York State's eJustice NY is currently in 800 sites with 8000 users; Pennsylvania JNET has become a nationwide model; while Washington D.C.'s JUSTIS, Colorado's CICJIS, and Maricopa County Arizona's ICJIS have also had significant success. Drawing on the work undertaken in these jurisdictions, New York City would benefit from established best practices and the increasing availability of products to support data integration.

Bottom Line

Reengineering DataShare and leveraging new technologies would create opportunities for cost savings and efficiencies. Though further study is required to identify cost savings, moving DataShare off of the existing mainframe could itself provide substantial savings. Also, numerous miscellaneous data lines between agencies could be consolidated. With more complete and timely information, City incarceration costs could be more tightly controlled.

The technology exists to meet the Executive Council's information sharing goals. It is anticipated that the replacement to Datashare -- a federated/distributed system, relying on a central hub and preserving the control of data at individual agencies -- could significantly extend the functionality of data sharing resulting in enhanced business practices that would lead to improvements in public safety.

Introduction

Designed by City criminal justice agencies, the Office of the Criminal Justice Coordinator and DoITT in 1995, DataShare enables City and State criminal justice agencies to share information through a "hub and spoke" architecture. In this framework, agencies connect to a central hub at DoITT, which enable them to send and receive data from all connected agencies via a single network line through the DoITT mainframe.

These exchanges are governed by the DataShare Executive Council, which has been working together for 8 years to improve the amount and quality of information sharing within the City criminal justice system. Working through the Executive Council, City and State criminal justice agencies have established protocols that govern what information is shared and with whom. The Executive Council also sets priorities for new projects. The existing DataShare program has been a success, facilitating the processing of hundreds of arrests every day. Yet over the years, several shortcomings have also become apparent.

In January 2003 the Executive Council determined that the current DataShare infrastructure was insufficient to meet the growing demands for data integration. As the criminal justice agencies bring new, up-to-date information systems on line, the ability to share increasing amounts, and increasingly complex types of data is restricted by the "mainframe" DataShare infrastructure. As needs are evolving, the existing DataShare tool is preventing the agencies from achieving their information sharing goals. After studying some of the integration efforts occurring in other jurisdictions (see Appendix A for a description of the progress made in other jurisdictions), the Executive Council convened a Subcommittee to determine the feasibility of using new technologies to expand integration between agencies.

This is the final report of that Subcommittee.

Section 1: Requirements

In order to establish a direction for its efforts, the Subcommittee began by defining a Mission Statement, detailing the functionality that a replacement system would offer, and describing the attributes that would guide the system's development and implementation.

Mission Statement

Controlled sharing of information within and between agencies to improve the efficiency and quality of the criminal justice system.

Functionality

The Executive Council established the functionality described in the following table:

Function	Description	Example
Production (Push)	Business rule-based sending of data from one agency to another	NYPD sends information about an arrestee to district attorneys
Query (Pull)	Searching another agency's database for information that would be displayed on a web page or incorporated into another agency's database	Searching DOC's database to determine if an individual is in their custody and displaying that information on a web page
Notify	Subscribing to be notified about a criminal justice event	Probation officer subscribes to receive an email notification when one of their probationers gets rearrested
Share Objects	Sharing digitally signed documents, images, and sound files	NYPD transmitting DV photos to district attorneys
Report	Getting aggregate data for research purposes	What's happening in Community Board 3?

Four Examples of Functionality
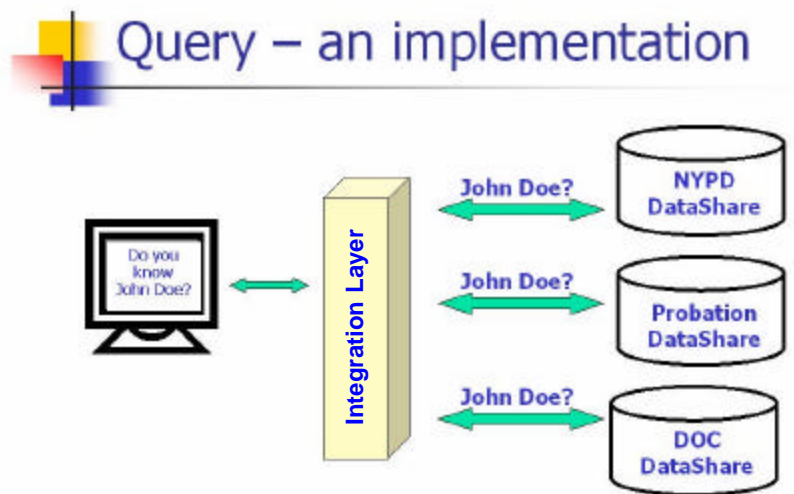
Query – an implementation

A criminal justice practitioner makes an electronic request for information from another agency. The central hub confirms that the user is authorized to receive this information (authentication) and the requested information is posted to a secure web page.

Push – an implementation
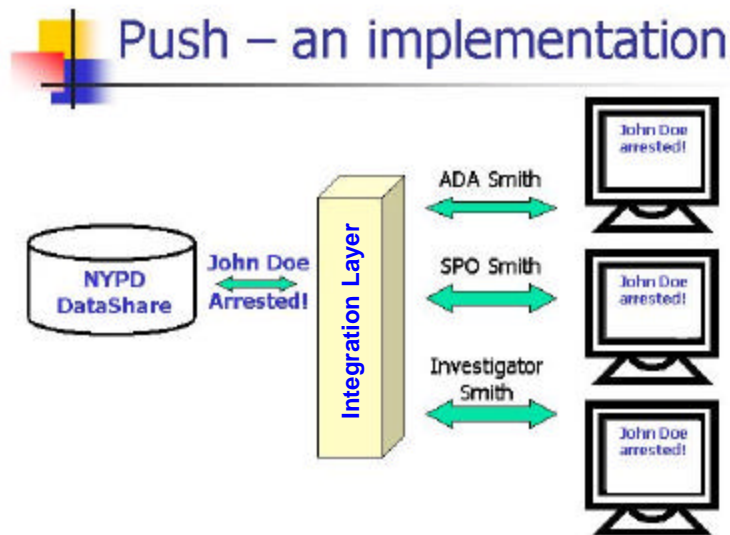
A predefined automated process to push data from one agency to another. Such as the NYPD pushing arrest data to the district attorneys after booking.

Four Examples of Functionality (cont.)

Pull – an implementation
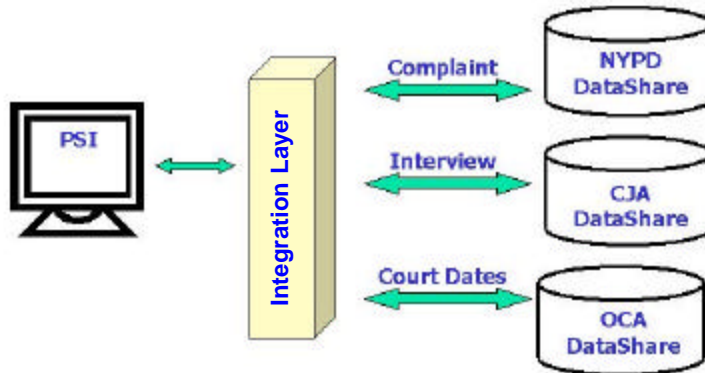
A criminal justice practitioner makes an electronic request for information from another agency. The user is authenticated and that information is pulled into and displayed in the user's case management system.

Subscribe – an implementation

A criminal justice practitioner subscribes to receive an automated notification via email, phone, or pager upon the occurrence of a criminal justice event.

Attributes

The Subcommittee established the attributes described in the following table:

Attribute	Description
Secure	Data, and the communications of it, must be secure, with the originating agency retaining ownership, including the ability to designate who can access it. (DoITT is now implementing Lightweight Directory Access Protocol (LDAP), which will serve as a common way to identify and authenticate users and determine which functions and information they should have access to.)
Consistent	Data should be consistent when possible, recognizing that agencies do not currently adhere to the same data standards. Efforts should be made to encourage compliance with recommended formats.
Accurate	Data should be entered and delivered accurately, and participants should provide indication or description of known inaccuracies.
Timely	Data should be made available in a timely basis. The goal of the system should be near real-time for delivery of all information when possible.
Usable	Data should be delivered in a way that makes it useful.
Adaptable	The system should be able to change with the City's changing needs.
Skill Center	The City must possess the skills to make changes to the system and should not need to rely on a consultant for changes.
Autonomous	The system must recognize the autonomous nature of its players and the data that each produces, it is recognized that each agency must consider its own operating priorities when determining when, where, and what data is captured and shared.
Performance	It must be recognized that performance of production systems for internal operation is the first priority of participants and any solution must not adversely impact that performance.
Transformation	The system should have the ability to transform data formats from one format to another so that each agency does not have to do the transformation themselves.
Fault-Tolerant	The infrastructure should be disaster resilient, as agencies will increasingly rely on it for mission critical communications.

Section 2: Existing NYC Criminal Justice Information Sharing Tools

In order to establish a baseline, the Subcommittee discussed the DoITT maintained tools used by New York City criminal justice agencies. Although primarily focusing on DataShare, the Subcommittee also examined the City's CityNet network and the applications available through CityNet, as well as the newly implemented 911 Call Delivery System which utilizes TCP/IP standards. The Subcommittee examined these systems relative to functional requirements designated by the Executive Council and also examined the architecture and strengths and weaknesses of these systems.

It is important to note that in addition to these DoITT maintained multi-agency systems there are numerous external modes for accessing and exchanging data that are critical to the current functioning of the criminal justice system, for example: most City criminal justice agencies access DCJS eJustice NY through a secure network connection; NYS Division of Parole provides data on a per agency basis via individual (dial-up) connections; in some instances individual agencies exchange data of interest via alternative channels (i.e. NYPD provides their service roster database to district attorneys on CD-ROM). These components, and the function they provide, should be considered as part of the integration requirements. The integration of the information currently obtained from these disparate systems can provide significant potential savings and benefits.

One significant hurdle addressed by the current information sharing situation is the established network infrastructure that has resulted – every agency involved currently has some communication capability with DoITT: whether via CityNet or the Financial Management System (FMS). The groundwork required by any integration effort has been laid, greatly easing the burden of implementation.

DataShare

Designed by participating agencies, the Office of the Criminal Justice Coordinator and DoITT in 1995, DataShare enables the automated sharing of data between City criminal justice agencies, both at the City level (mayoral and non-mayoral) and at the judicial level (Office of Court Administration New York City Criminal and Supreme Courts).

Data sharing is accomplished by loading DataShare software on CityNet connected PCs at participating agencies. At a "sending" agency, data is extracted from the agency's files and transmitted and temporarily stored at the DoITT mainframe. The DataShare PCs at the designated "receiving" agencies in turn download the files when available. Receiving agencies can then load the data into local files for use in individual systems.

DataShare utilizes a very traditional and tried-and-true method for sharing data: strings of data are pushed from agency to agency using a series of interconnected main-frame connections. Agencies that receive data through DataShare then develop a batch process to integrate these strings into their own databases. When a sending agency changes the format of the data they distribute, each of the receiving agencies must subsequently reprogram their batch processes to reflect the new format of data they receive. The system is not a data warehouse but acts only as the central distribution system.

Currently, DataShare transmits New York State Criminal Court and Supreme Court data, NYPD arrest data, Department of Correction data and minimal Criminal Justice Agency data. When implemented in 1995, it was anticipated that more data would become available via DataShare, but this did not occur due to the complicated tools associated with the DataShare system.

In order to gauge the potential for additional information sharing, the Subcommittee surveyed participating agencies for a list of applications and infrastructures currently participating in DataShare and that could be added to DataShare (see Attachment B). The results of this survey were encouraging, illustrating that those agencies responding generally utilize, or plan to migrate to, standard internal network protocols, and are using relatively current, capable database platforms. It was also determined that all agencies are either now, or soon will become, part of the City's TCP/IP network. This network will provide the pathway between data sharing and the individual agencies.

This survey, which should be expanded to include all member agencies and all applications that could be of interest to other agencies, also indicated that there is opportunity for expansion; 12 of the 21 applications submitted by the 10 responding agencies do not currently participate, but could if desired.

The Subcommittee also evaluated the strengths and weaknesses of DataShare. Significantly, prior to the implementation of the existing DataShare system there was extremely limited information sharing between criminal justice agencies. As a result, an important strength of the existing system is that it facilitates the transfer of a large volume of essential data between many of the agencies in the New York City criminal

justice system. This data is used every day to process hundreds of arrests, prepare cases for court and manage defendants who are incarcerated. Yet as important as the present DataShare functionality is, the system is extremely limited when viewed in the context of information that agencies wish to but cannot now share because of DataShare's shortcomings.

The diagram below illustrates the direction of data flow, the topology and protocols currently used, and in the case of NYPD, the data availability frequency. The architecture of the existing system conceptually mirrors a hub and spoke integration model. It serves essentially as a batch file transfer infrastructure, with no added intelligence.
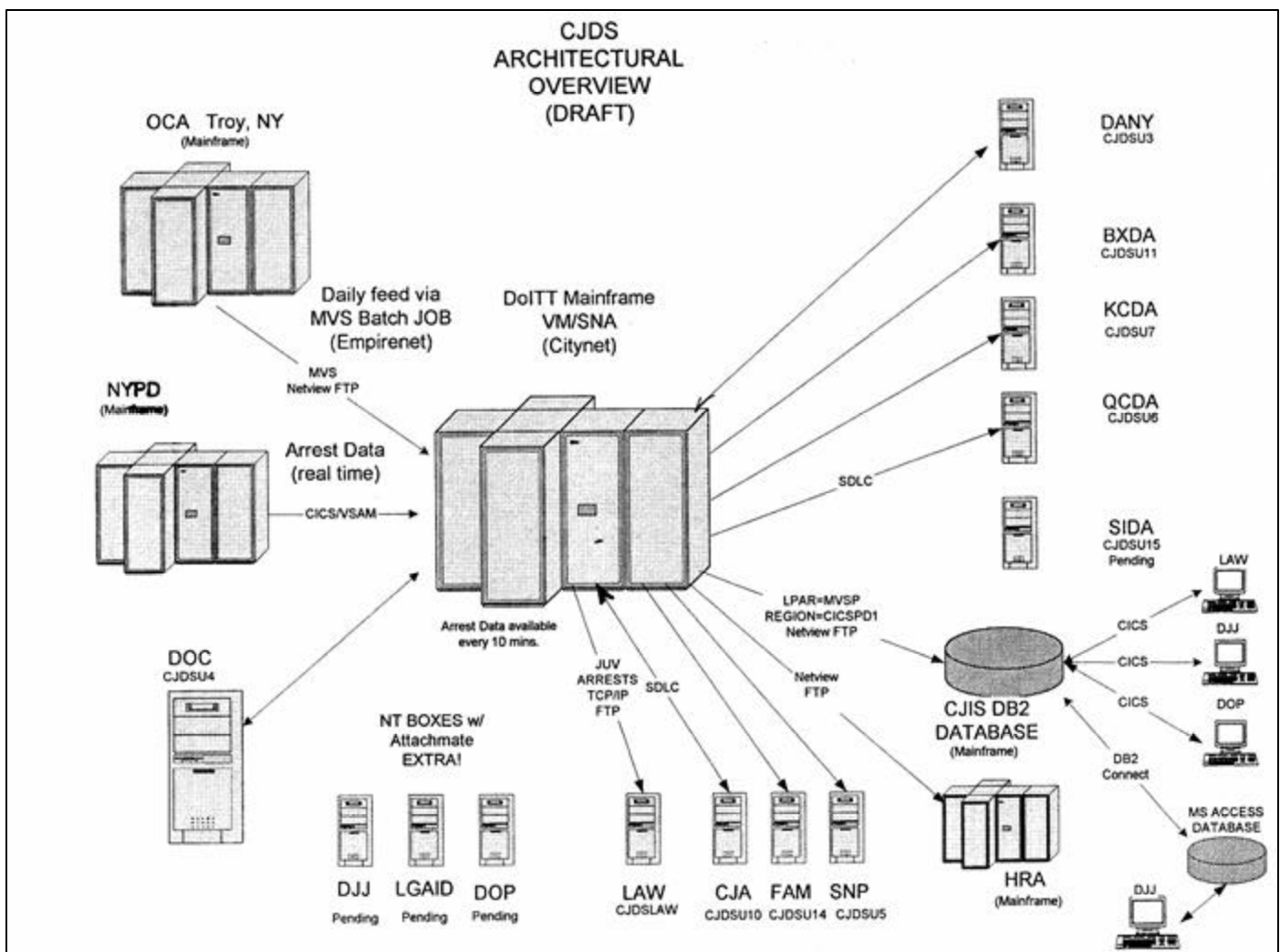
Strengths of DataShare

Area	Issue
Security	Mainframe based authentication of defined user accounts via SDLC. Agencies maintain control over which agencies receive their data.
Reliability	While not fault tolerant, DataShare has run reliably for years with minimal interruption. Agencies have confidence in the reliability of DataShare and thus have been able to incorporate the information they receive into their daily business processes.
Compatibility	The existing architecture, while based primarily on the mainframe SDLC transport protocol, does support the more commonly used TCP/IP network communication protocol.
Content	The content currently available is extremely valuable and heavily relied upon by participating agencies. Providing agencies with access to this data has decreased some duplicative data entry associated with arrest and court information.
Efficiency	DataShare provides agencies with access to data from multiple sources through one line as opposed to requiring agencies to purchase and maintain multiple connections in order to receive this data.

Weaknesses of Datashare

Area	Issue
Functionality	Only addresses one of the Executive Council's five integrated justice requirements – Production.
Adding Data	In adding data from existing systems to DataShare, originating agencies need to "dumb down" the data into string-format. This is time consuming and the transmitting agency has less of an incentive to put the time in to make the data transferable.
Using Data	Data is difficult to work with and is time consuming to incorporate into agency databases. As a result, some agencies lack the technical resources to utilize the data.
Inflexible	Responding to additions and changes to data is difficult. Each time an originating agency makes a change to their system, the format of the file changes as well. Each agency, on multiple platforms, has to individually modify applications and data transformations in order to make use of changes in information available.
Lack of Fault Tolerance	While very reliable, there is no provision for fail-over in the event critical components are unavailable. Also, since the technology is no longer industry standard (main-frame), trouble-shooting can be difficult.
Transformation	The system does not have the ability to transform data formats from one format to another but requires that each agency perform their own transformations from the unusable transmitted string-format to their own internal storage means (e.g. tables).
Lack of Data	Each agency uses their own database platform, data architecture, and

| Standards | development environment. While New York State publishes the Statewide Criminal Justice Data Dictionary, few agencies adhere to this standard. In addition to the NYS standards, there are currently several published national standards for criminal justice integration efforts. Virtually all of these standards utilize the extensible markup language (XML) as the core data format. |

Finding: DataShare has improved the amount of information sharing within the criminal justice system. However, DataShare is outdated and does mot meet the City's "production" functional requirements. Sending agencies have to convert their native data to text format and receiving agencies have to convert the received text to their native format. This is terribly inefficient and stifles information sharing within the New York City criminal justice system. Moreover, the additional functions envisioned by the Executive Council other than production are not possible using the existing DataShare infrastructure.

CityNet Applications

CityNet is the DoITT maintained network used to provide access to applications throughout the City. City agencies can access numerous legacy systems via this network. Those used by the City's criminal justice agencies are listed below. Additionally, there are several criminal justice applications that although currently not available, would be widely used if they were available via CityNet.

CityNet is an extremely valuable resource that attempts to satisfy the pull, or inquiry needs of criminal justice agencies. However, it does so in a manual case by case, system by system retrieval method.

Applications Accessed by Criminal Justice Agencies via CityNet

AJIS	ADULT JUSTICE INFORMATION SYSTEM
CJIS	COMPREHENSIVE JUSTICE INFORMATION SYSTEM
CRIMS	OCA NYC COURT CASE TRACKING
BADS	NYPD BOOKING/ARRAIGN/DISPO SYSTEM
CACS	NYPD APPEARANCE CONTROL SYSTEM
OLPA	NYPD ON LINE PRISONER ARRAIGNMENT
BXDA	BRONX DA CASE TRACKING SYSTEM
CAR	DMV: DEPARTMENT OF MOTOR VEHICLE
CAMIS2	NYC DEPARTMENT OF CONSUMER AFFAIRS
CCIS	CIVIL COURT INFO
DOB	BIS: BUILDING INFORMATION SYSTEM
VEND	NYC VENDEX: OFFICE OF CONTRACTS
GEO	GOAT: GEOSUPPORT ADDRESS TRANSLATOR
HPD	PREMISYS MULTIPLE DWELLING DATABASE
LAW	NYC LAW DEPARTMENT BRIEF BANK
JDLS	JUDGMENT DOCKET & LIEN BOOK, NYC
DOF	NYC DEPT OF FINANCE MORTGAGE/DEED
ARCS	NYPD AUTOMATED ROLL CALL SYSTEM
LUMIS	CITYWIDE LAND USE/ULURP SYSTEM
MISLAND	CSC: MISLAND SYSTEM

Strengths of Applications Available via CityNet

Area	Issue
Content	There is a wealth of information available via CityNet.
Security	Although cumbersome, security through individual passwords for each application ensures that unauthorized users cannot access these applications.
Reliability	CityNet is extremely reliable.

Weaknesses of Applications Available via CityNet

Area	Issue
Functionality	CityNet does not permit simultaneous querying of multiple systems or the ability to "pull" data from another agency's database.
Usability	Logging in and out is extremely cumbersome as a different password is required for each application. Users must also learn the various key-strokes of these mainframe applications. These key-strokes are difficult to learn and prevent users from utilizing these applications.
Inflexible	Only legacy systems are currently available via CityNet.
Criminal Justice Content	Very few core criminal justice applications are available.

Finding: The applications available through CityNet provide data that is used by many agencies. We should explore using this resource to provide access to more core criminal justice applications. Most significantly, CityNet may be used as the backbone for a new application that would allow criminal justice practitioners to query multiple systems simultaneously through a browser front-end and single sign-on.   Or in the alternative, where agencies would prefer to "own" the data, they would pull the data from other systems for display in their own application (Query function).

CityNet 911 Call Delivery System

Currently being implemented by DoITT, the NYPD and the district attorneys, the 911 Call Delivery System is used to transmit 911 calls from the NYPD 911 call recording system to assistant district attorneys. When a requested call is located in the 911 call recording system by an NYPD technician, it is posted onto a portal server for assistant district attorney retrieval. An email notification is simultaneously sent to the assistant district attorney that requested the call, informing the assistant district attorney the request has been fulfilled. By clicking on an imbedded URL in the email, the district attorney is taken to a secure intranet portal where she can download the call. Assistant district attorneys can also access fulfilled requests by logging onto the portal.

To ensure security, the files are encrypted prior to being transmitted. They are automatically decrypted upon receipt. The system also digitally signs all calls in order to ease the admissibility of the electronic recording as evidence at trial. An NYPD certification indicating the contents of the transmission and containing an electronic signature from the technician that fulfilled the request is also included. The calls are converted from wav to MP3 format for transmission and storage efficiency as well as higher play back compatibility with commercially available compact disc players. The portal is supported by a Windows 2000 Server-based Web server infrastructure.

Access to the portal is through CityNet and this is the only criminal justice TCP/IP application accessible via CityNet. The 911 Call Delivery System is an example of an application that could only be developed utilizing this modern network TCP/IP protocol and its available software development tools.

Phase 2 of the project will include the creation of a call request tool using Siebel customer relationship management software. Assistant district attorneys will be able to submit requests for 911 calls to the NYPD and check the status of requests, via a portal. Phase 2 should be completed by late September '03.

Strengths of the 911 Call Delivery System

Area	Issue
Authenticity	Call authentication ensures the file has not been altered and makes the admissibility of the call at trial easier.
Security	Only the requesting assistant district attorney can access his/her fulfilled request.
Timeliness	Email notification informs assistant district attorneys that their requests have been fulfilled.
Usability	Browser based front-end and conversion of file to widely used format that takes up less disc space result in a user-friendly product.
Extensibility	Built to be expanded to provide increased functionality.
Portability	The 911 Call Delivery System is platform independent.

Weaknesses of the 911 Call Delivery System

Area	Issue
Functionality	Only shares 911 calls between NYPD and assistant district attorneys.
Transferability	Vendor created, thus improvements to the system will be difficult unless City obtains additional resources.
Support	City does not have the skills to support the system.

Finding: The 911 system is an excellent first step toward providing the "Share Objects" requirement set forth by the Executive Council. The possibility of leveraging this tool to extend it to other objects such as PDFs and digital photographs should be explored. The City should also consider acquiring in-house skills to ensure that the system continues to evolve to meet the user's changing needs. Extending Phase 2 functionality to other interagency criminal justice requests should also be considered.

Section 3: Needs

The Subcommittee explored various integration approaches that could be applied to our objectives to evaluate applicability. These models included a data transfer/integration/transformation engine, a portal/reporting package, and a guaranteed-delivery messaging architecture.

These requirements were considered in the context of the current business needs of the NYC criminal justice community in scenarios distilling the abstract into the practical. A series of scenarios were identified that would test a wide range of technical challenges that these objectives might offer. The scenarios do not necessarily represent specific projects that the Executive Committee might choose.

Objective: Production

Scenario: Receive Omniform[2] data for all new arrests

The current feed of OLBS data is exceedingly small in comparison with the contents of the Omniform data. If we were to use the current data sharing architecture to facilitate the transfer of Omniform data for all new arrests, we would have to continue the outdated practice of transmitting strings of data.

Transmitting strings of data is more than a bit inefficient since the NYPD Omniform file structure is already similar to other systems maintained by the criminal justice community. The NYPD uses a modern and standard table view of the Omniform data (e.g., different data elements are categorized into separate entities and are linked together by unique numbers, namely complaint and arrest numbers). This standard structure makes access fairly straight-forward and is facilitated by tools that range from free (e.g., ODBC - a standard system interface) to only moderately more expensive (e.g. messaging tools).

However, if the NYPD were to use the existing DataShare architecture, they would have to invest time in stripping the rich Omniform data down to strings. In turn, most recipient agencies would need to raise the bar back up to convert the string data to their own structures -- structures probably similar to the NYPD's native structure.

If newer technologies were used, NYPD would be able to "expose" their data in any desired format and agencies with permission to do so would be able to retrieve the data in any desired format.

---

[2] Omniform is the new TCP/IP browser based system used by the NYPD for Arrest and Complaint information. It is the consolidation of two systems, the Online Booking System ("OLBS") and the Online Complaint System ("OLCS"). OLBS and OLCS continue to operate and are populated via data entry into the Omniform system.

Finding: The current DataShare system does not have the capability to send data in any format besides text strings. Agencies have to convert their native data to text format. Receiving agencies have to convert the received text files to their native format. This is terribly inefficient. By using new technology we would eliminate the barriers agencies face when trying to contribute data to DataShare and therefore create numerous information sharing opportunities.

Objective: Query

Scenario: Create a single inquiry that would combine Omniform data with data from another source, for example, Department of Correction inmate data.

As explained above, the current data sharing data files are simply strings of data. These files are created independently across different agencies (e.g., NYPD and DOC) without any standard structure or enforced common fields (e.g., arrest number). By the very nature of this format, it is impossible to easily link different sources of data and inquire on the results. Instead, agencies must first import the data into their own databases, merge the data, and program their own inquiry functions.

Using new technologies, however, inquiries could be developed centrally - at the portal level. There users could enter one of several indices (e.g., NYSID) and the central messenger could access data from multiple sources (in this example: NYPD and DOC). The messenger would then cull through the data and provide the user with the results from all databases in one formatted display.

Finding: The current data sharing process provides a series of data files from different agencies that are not linked in any way. It is the responsibility of each agency to link the data and present it to the user. Using new technologies, single central inquiries can be developed that different people and systems can use and re-use.

These queries would be accessible via a browser that would have point and click functionality as opposed to the difficult to use interface currently used to access legacy systems. The queries would also be accessible directly by systems, whereby an agency case management system would be able to "pass" specific requests to the DataSharing portal. The portal would then return data back to the agency's system for display to the user.

Objective: Notification

Scenario: Automatically generate notices of arrest for particular defendants.

Right now the DA offices receive data files from the NYPD for all arrests made in their respective counties. Other agencies (e.g., DOC) receive all city-wide arrests. Each receiving agency tends to examine the arrests, looking for particular new arrestees. For instance, the Department of Probation needs to know about new arrests involving current probationers; the DA offices needs to know about rearrests involving defendants who

may have other pending cases; many different parties may need to know about "Operation Spotlight" arrestees.

Each agency is currently responsible for processing arrest data and programming matching criteria against their own "watch" group. This is not always a simple task and is not being done by all agencies. And even when done, the data is limited to just those arrests that the agency is aware of (possibly, only their particular county).

With new technology, the middleware could be responsible for monitoring all new arrests appearing in the Omniform system and matching these arrestees against various different "lists" of defendants. Using technologies unavailable now with Data Sharing, the lists could be maintained in different ways, according to agency capabilities and circumstances. For instance, a small agency may choose to manually enter the individual "watch" people into a browser application, while another agency may choose to expose a data table of "watch" people to the middleware.

Furthermore, newer technologies allow for various distribution methods. These may range from e-mail transmissions to pager notifications. Some agencies may also wish that the hits be transmitted to their own data bases so that the data could be coupled with their own internal data and formatted in particular ways to particular people.

Finding: The current data sharing process does not inherently contain the capability to examine data to identify particular events nor does it have the means to communicate to users via different distribution methods (e.g., e-mail). Modern middleware and a simple application would enable the City to accomplish the notification function.

Objective: Share Objects

Scenario: Users wish to access the DCJS eJustice Rap Sheet when accessing the Omniform data.

There is currently limited facility to share object data (e.g., pictures, sound files) throughout the criminal justice system. The new architecture, would treat object data no differently than it treats traditional data such as defendant name or arrest date. One example of object sharing could be an arrestee's rap sheet.

While the DCJS eJustice rap sheet system provides new fingerprint-based rap sheets in a very timely fashion, access to rap sheets is currently limited to a relatively awkward process where users have to monitor a list of new raps in an eJustice In-Box. If DCJS were able to push down the rap sheet "objects" to a table linked to the PD Omniform system, systems and users could have "one-stop-shopping" when satisfying crime and arrest data needs.

There are numerous ways that this could work. The following is one illustration. When DCJS creates new In-Box entries, DCJS could also create Adobe PDF file images of the rap sheets. These files – named with the arrest numbers – could then be transmitted to either a DOITT sever or directly to the PD Omniform system. Flags would then be set to indicate which files are new and notifications or pushes could be made to the respective agencies. Agencies could then access the rap sheet images using the same or similar mechanisms as those established to access the Omniform data.   When subsequent out-of-state hits are found, follow-up transmissions would be sent and the flags would again be set to "new rap". The Adobe PDF file format is identified here since the viewing software is free and the produced documents are unmodifiable.

Finding: There is currently limited facility to share objects (e.g., pictures, sounds) throughout the criminal justice system.   If rap sheets were available as objects to be shared, systems could have the same access to an arrestee's prior criminal history as they would to any other data.   The new architecture, would treat object data no differently than it treats traditional data such as defendant name or arrest date.

Objective: Reporting

Scenario: Users wish to see the number of new arrests for the previous week based on county, charge, precinct of arrest, or Community Board.

There are numerous relatively inexpensive reporting tools (e.g., Crystal Reports) that allow for the development of reports presenting lists, cross-tabs, and graphical reports. Other software, like MapInfo, can present geographical data in maps showing gradations of, for instance, severity of crimes. Still other software, like SPSS, provide functions to perform detailed statistical analysis apart from standard descriptive statistics such as average or median.

These reporting tools, as well as other types of software (e.g., forms generation, spreadsheet) require data to be in one of several standardized formats. The formats that can be "exposed" to the reporting tools include objects, tables, XML (a modern file sharing format) and certain prescribed text file formats. The drivers – the software that sits on PC 's – that talk to the reporting packages are usually free or very inexpensive.

The current data sharing files are not generated in any of the standard formats. There are no available drivers that allow reporting software to speak to the current data sharing format. Instead, the files must be reformatted and usually merged into existing data base applications before the data could be used by the reporting tools.

Using the example above, agencies could access the Omniform data either through a direct connection to the PD database or to sub-sets that might reside locally or on a DOITT server.   Under the planned architecture for a new system, the data formats will be modernized so that reporting tools could point directly to the data, no matter where the data resides.

Finding: The current data sharing format is not compliant to standard reporting software and must be re-formatted by custom applications and tools before it can be used by reporting tools. Modern data-integration middleware would allow data that resides in various applications and platforms to be available in a consistent format and taxonomy. This would ease the data cleansing burden on agencies while also enabling the creation of reports across data from multiple agencies (e.g. NYPD arrestees, DOC inmates, DOP probationers).

Section 4: Implementation

While configurations differ somewhat depending on the specific products or suite chosen, a generic integration approach providing the required features would consist of: a component at the edge of each participants' database(s) or application, connected to a central integration server, as illustrated on the following page. These edge components would provide the communication interface, including security, required for the transfer and messaging elements. The edge components might also contain aggregated, normalized data for management analysis and reporting.
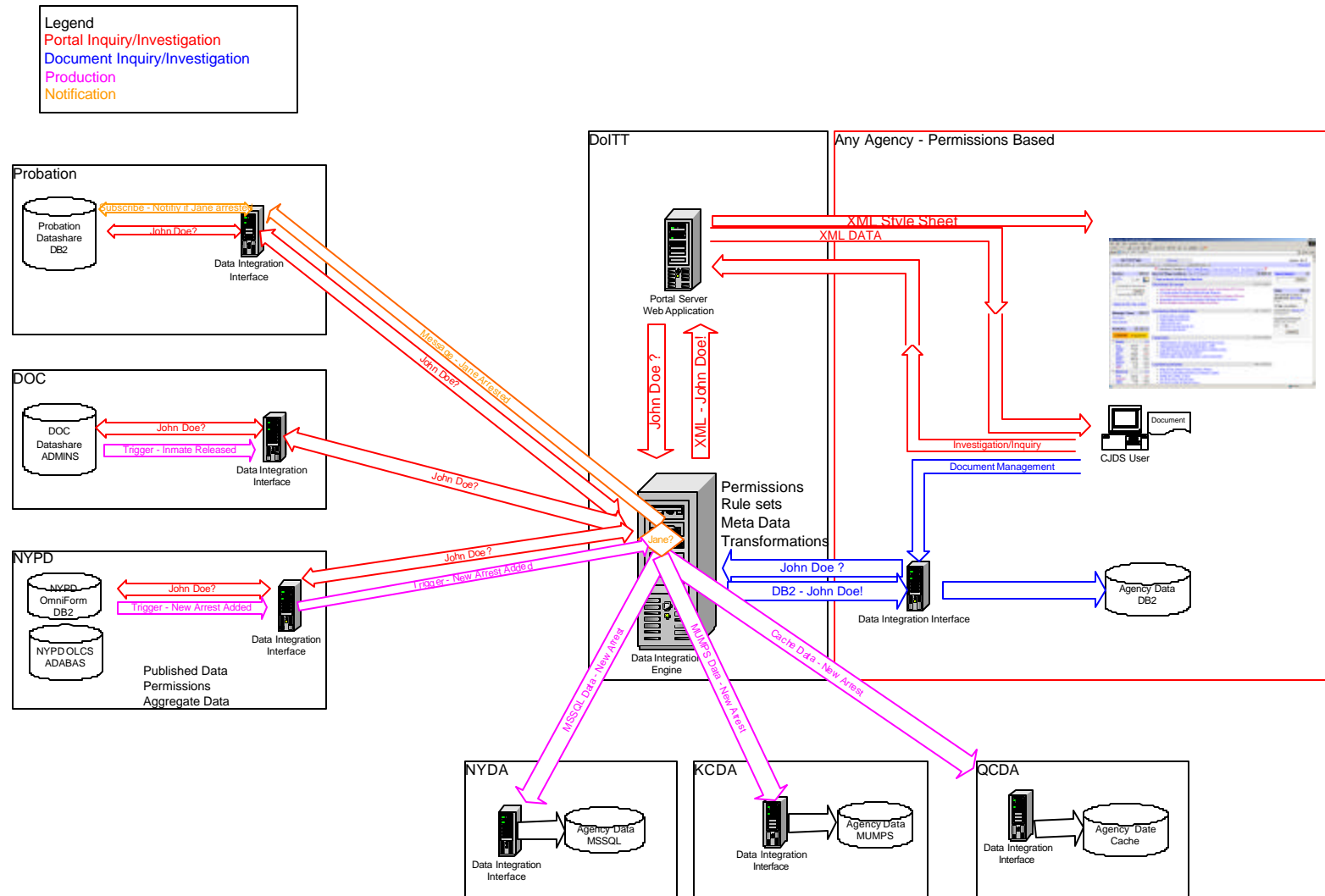
The central component would provide the transformation of the data and messages from one format to another, supplying it to targeted recipients in the desired format. This central component would be the repository for rules defining what agencies had access to what information, and when. It would also supply the information to the central portal application that serves up integrated responses to inquiries.

Potential Benefits

Aside from the benefits achieved to participating agencies' systems, there are ancillary benefits to improving DataShare as well. Concentrating valuable technical skills at a central point – the integration hub – and making them available to those agencies that do not have the resources – better leverages them. By maintaining a central web based portal retrieving data from, and being used by, multiple sources including police, courts and correction, greatly benefits smaller agencies who do not have in-house systems. A portal approach would provide immediate access to new data by implementing change in a single application, while preserving each agency's ability to incorporate that additional information into their internal systems as they see fit.

Currently, each of the participating agencies have connections over various protocols through DoITT for the existing DataShare as well as other applications. In many instances agencies also have point-to-point connections with multiple other agencies as well. Often these connections run over frame relay, fractional, or full T1 leased circuits. Reviewing and consolidating them to run on a central protocol over CityNet would facilitate DataShare, and potentially reduce recurring telecommunications costs. Where interagency connections remain, they can be configured to provide redundancy and fault tolerance for DataShare.

Illustration of Network Architecture

Legend
Portal Inquiry/Investigation
Document Inquiry/Investigation
Production
Notification

Probation

Probation Datashare DB2

Subscribe - Notify if Jane arrested

John Doe?

Data Integration Interface

DOC

DOC Datashare ADMINS

John Doe?

Trigger - Inmate Released

Data Integration Interface

NYPD

NYPD OmniForm DB2

John Doe?

Trigger - New Arrest Added

NYPD OLCS ADABAS

Data Integration Interface

Published Data
Permissions
Aggregate Data

DoITT

Portal Server
Web Application

XML Style Sheet
XML DATA

John Doe ?
XML - John Doe!

Permissions
Rule sets
Meta Data
Transformations

Jane?

John Doe ?
DB2 - John Doe!

Data Integration Interface

Data Integration Engine

Any Agency - Permissions Based

Investigation/Inquiry

Document

CJDS User

Document Management

Agency Data DB2

Message - Jane Arrested
John Doe?
John Doe?
John Doe ?
Trigger - New Arrest Added

MSSQL Data - New Arrest
MUMPS Data - New Arrest
Cache Data - New Arrest

NYDA

Data Integration Interface

Agency Data MSSQL

KCDA

Data Integration Interface

Agency Data MUMPS

QCDA

Data Integration Interface

Agency Date Cache

Products

There are numerous products available in the category of integration software, including IBM Websphere, BEA Systems WebLogic, and DataJunction. In addition, many of the database platforms currently in use by participating agencies include built in support for integration and exchange of data with external system. Reporting software such as Crystal Reports will probably also be incorporated into the middleware so that some data could be reported in graphics or statistical tables. A detailed requirements document can accurately estimate the cost of implementation. This requirements document, including the features identified by the committee to-date, must be created and thorough product evaluations performed. In addition to the integration software, there will be consulting and hardware requirements as well. Finally, the use of open source software should also be explored in order to minimize costs.

None of the solutions reviewed are a panacea or silver bullet, and all would entail substantial work to implement. For all of the glossy advertising by the product manufactures touting their products as "automatic enterprise data integration tools", there is significant complexity in mapping data transformations and creating rules for integration to work seamlessly.

The recommended approach would result in a shifting of this responsibility from the individual participating agencies to the central hub, which would be the responsibility of all of the participating agencies as well as DoITT. The work there involves creating and maintaining complex data transformations, establishing the rule sets for notifications, and maintaining permissions among other tasks.

The committee has received extensive information on some of these products and generally confirmed their ability to provide functionality described herein, but has not itself evaluated any specific brand. Many of these integration packages and other required hardware and software are available under the NYS Requirement Contract, and some may be available under the NYC Requirement Contract, and could be procured expeditiously.

Section 5: Conclusions

The Subcommittee has concluded that technical solutions are available to meet the broad objectives established by the Executive Committee.

Specifically, the committee recommends that:

1. The existing DataShare architecture, consisting of a central infrastructure, be updated with new middleware in the form of enterprise integration tools which provide existing functionality and add the new desired features.

2. The technology should be built on a TCP/IP network and accessible to users via a user-friendly browser based front-end (a NYC Public Safety Portal). The same types of inquiries should also be able to be done directly by agency case management systems, so that there may be seamless integration between existing systems and the middleware tool.

3. Levels of integration beyond simple data exchange (i.e. One of the Executive Council's five functions, such as pulling data from one agency to another on an as needed basis) should be implemented in an effort to improve the quality and usefulness of the DataShare initiative.

4. XML standards governing data and entity elements should be endorsed as a recommended architecture for participating agencies, and NYC DataShare should actively participate in the further development of these standards. A determination will be made as to the source of the standard (e.g, DCJS).

5. All member agencies should be surveyed to gather detailed information on those applications that participate in, or could contribute to, the DataShare initiative.

6. Next steps should include preparing documentation for OMB, continuing to refine business and infrastructure requirements, and preparing documents to go out to bid. Specific high-value integration projects should be identified based on cost and public safety benefit.

Exhibit A: Leading Criminal Justice Integration Efforts

Jurisdiction	Accomplishments
New York State	eJustice NY is New York State's criminal justice portal. eJustice NY is used by most City agencies to make criminal justice history inquires (Query), which are returned via a user or agency eJustice NY inbox. (http://criminaljustice.state.ny.us/index.htm)
Pennsylvania	JNET facilitates Push, Query, Picture Sharing and Notification. Next steps include the addition of digital certificates. (http://www.pajnet.state.pa.us/pajnet/site/default.asp)
Washington D.C.	JUSTIS enables users to access 17 sets of data from 13 agencies including documents and images. Facilitates Production, Query, Notification and Object Sharing. (http://www.cjcc.dc.gov)
Colorado	CICJIS facilitates Push and Query. (http://www.state.co.us/gov_dir/cicjis)
Maricopa County Arizona (Phoenix)	ICJIS facilitates Push and Pull with additional functionality planned. There is a full-time business analyst from every criminal justice agency dedicated to the project. (http://www.maricopa.gov)

The United States Department of Justice funds a national data integration clearing-house, maintained by the not-for-profit group SEARCH, inc. For a comprehensive description of nationwide criminal justice integration efforts see http://www.search.org/integration/state_map.asp.

Exhibit B: Sample Integration Projects

Below is a list of what could be accomplished in an integrated criminal justice system. Some of these scenarios may be applicable to New York City but are included only to give the reader a sense of what could be accomplished in an integrated criminal justice system.

Source: NASCIO (Available at http://www.nascio.org/hotIssues/justice/Fullrept.pdf)

The following is an example of how increased information data integration might work in the criminal justice context.

1. A suspicious police officer submits a query to the statewide warrant system and discovers from the response that the subject of his car stop is wanted.

2. A police officer arrests a subject, then completes and (digitally) signs an arrest document which describes the crime, arrest and arrestee, stores the document in the police information system, and finally affixes to the arrestee a bracelet containing the arrest document number.

3. The arrestee is taken to the sheriff's office to be booked. The sheriff's information system uses the arrest document number, scanned from the subject's bracelet, to pull the arrest document from the police information system, and uses data from that report to (partially) fill in the booking document.

4. The sheriff's information system, using personal-description data in the arrest report, pulls the local, state and national criminal history records, and, based on the information in these documents, a person who makes a security decision enters that decision into the sheriff's information system which assigns an appropriate cell.

5. The sheriff's information system uses information from the arrest and booking documents to fill in a standard press release and pushes it to the appropriate web page.

6. The sheriff's information system uses information from the arrest and booking documents along with the mug shot and electronic fingerprint capture submission, using live-scan or card-scan solutions, to push to the state criminal history repository the arrest report required. The state repository's information system will, after its own processing, push the information to the national criminal history repository maintained by the FBI.

7. The sheriff's information system pushes to the prosecutor's information system the arrest document, booking document and three criminal history records, and the prosecutor's information system uses some of this information to (partially) fill in a prosecution case intake document. An assistant prosecutor views all the available information and makes the decision to prosecute.

8. The assistant prosecutor decides the specific charges to be filed, and the prosecutor's information system prepares the charging document using statute-specific standard charging language plus information from the earlier police and sheriff's documents. The assistant prosecutor (digitally) signs the charges and the prosecutor's information system pushes the charges to the court's information system.

9. The court information system creates the initial records for a new case, assigns it, reviews the judge's calendar and sets a time for a preliminary hearing. It then pushes to the prosecutor's information system and the public defender's information system information concerning the assigned judge, courtroom, date and time. The prosecution's information system reviews its workload and fills in its calendar by assigning the hearing to one of its assistant prosecutors, and the public defender's information system similarly assigns the hearing to one of its defenders.

10. Throughout the course of the trial the prosecutor's and defender's information systems push digitally signed motions to the court's information system, the court's information system pushes copies of motions and notifications of hearings to the prosecutor's and defender's information systems, and the human parties, namely the prosecutor, defender, defendant and judge, meet and make decisions. At appropriate times, the court's information systems pushes notifications to witnesses who are required to attend a given hearing or trial portion, and the prosecutor's information system pushes notifications to victims at important milestones of the case.

11. At one point the defendant, who is free on her own recognizance, fails to appear for a court date and the judge issues and digitally signs a warrant, which the information system pushes

to the original arresting agency for service.

12. As the trial ends the judge decides the case and passes sentence, which the court's information system transforms into a (digitally) signed document which it then pushes to the sheriff's information system to send the newly convicted prisoner to the state prison, pushes another such document including the sentence ordering the prison's information system to receive the prisoner, pushes yet another document to the defender's information system setting the date by which a notice of appeal must be filed, and so on.

13. Later the prison's information system and the parole information system coordinate the transfer to parole.

14. Unfortunately, while on parole the subject commits a crime and is arrested. When the booking information system retrieves the criminal history record via electronic fingerprint transactions, it notices that the subject is on parole and that the parole agency has subscribed for news of any arrests during the time of parole. It pushes to the parole information system an arrest notification message. The parole information system then prepares a parole violation document and pushes it to the appropriate parole officer for consideration.

The example, up to this point, has shown only interactions among the governmental entities which are usually thought of as comprising the criminal justice system. But there are many other entities which are pulled into the criminal justice process. For example:
- Private defense attorneys;
- Jurors and potential jurors;
- Public and private schools (truancy, vandalism)
- Public and private half-way houses;
- Public and private diversion alternatives to incarceration;

- Fire and other Public Safety governmental components for combined operations;
- Alliances of nearby police agencies for combined operations;
- State and federal agencies for periodic reporting on local crimes, arrests, prosecution cases and outcomes, court cases
- and outcomes, prisoner populations, correctional supervision cases and outcomes, and many more.

Notice that in the examples an information system (really the business process which is incorporated into the information system) sometimes knows that information is required and pulls it without being asked by a person. Other times an information system knows that another system will need certain information and pushes it, without being directed to do so by a person. Still other times an entity knows that it would want to be informed if certain events happen to a certain person, and subscribes to such information, confident that if the event happens the entity which holds the subscription will publish a notification to the subscriber.

Exhibit C: Sampling of NYC Criminal Justice Applications by Agency

Organization	Application			
Name	Name	Application Type	Department	Use
NYPD	OMNIFORM	Arrest and Complaint Processing	Various	Tracks all arrests and complaints entered citywide
NYPD	Domestic Violence	Various	Various	Tracks all Domestic Violence incidents entered citywide
Correction	IIS	Inmate Tracking System	Various	Inmate tracking; jail management; population research
CJA	UDIIS	Pretrial Defendant Tracking System	Various	Community Ties Assessment, Scheduled Court Date Notification, ATIIS, criminal justice research
Probation	ARTS	Case Management	Adult Supervision	Adult Case Management
Probation	CJIS	Case Management	Family Court	Juvenile Case Management
DJJ	CJIS	Case Management	Various	Detained Juvenile Tracking
Special Narcotics	CIMS	Case Management	All	Court Case/Calendar Management
Special Narcotics	Search Warrants	Incident Tracking	Search Warrant Unit	Record issuance/execution/return & results of search warrants.
Special Narcotics	LABS	Lab Analysis Tracking	All	Request/Track status of requests for laboratory analysis of drugs/weapons
Special Narcotics	Investigations	Criminal Intelligence	SIB, Executive	Repository of detailed subject and activity relating to ongoing narcotics trafficking investigations.

| Organization | Application | | | |
Name	Name	Application Type	Department	Use
Queens County DA	Case Tracking	Case Management/Decision Support/Document Management via Arrest to Appeals tracking	All QCDA bureaus and 20 Queens police precincts/commands	Case management; document management; statistical reporting; mapping. Application also includes Complaint Typing (NYPD accessed) and Indictment Typing components.
Kings County DA	Case Tracking System	Case Tracking	All legal bureaus and limited office staff	Case Tracking - progression of a case through the court system
Kings County DA	Arrest to Arraignment System	Case Tracking	All legal bureaus and limited office staff	Initial case and Defendant setup
DANY	AJIS	Court Case Tracking	Office-wide	Case Tracking System
DANY	APS	Arrest Processing System	Complaint Room/Office Wide	Arrest Processing, Arraignment data entry

Organization Name	Application Name	Application Type	Department	Use
DANY	DANY Case Information (DCI)	Case Tracking	Office-wide	Case tracking, data warehouse, reporting engine
DANY	Indictment Processing System (IP)	Case Tracking	Office-wide	Grand Jury tracking, automated Indictment generation
OCA	CRIMS	Case Tracking	Various	Processes all stages of criminal case actions, from docketing in Criminal Court to final disposition in Supreme Court. Produces an extensive array of operational and administrative reports. Transmits data to DCJS for posting on rap sheets.
OCA	SAMS	Case Tracking	Various	Tracks universal summons cases processed in the Criminal Court, from docketing to final disposition. Handles scanning of summons forms. Provides a Cashiering function and produces numerous reports.

Organization Name	Application Name	Application Type	Department	Use
OCA	UCMS	Case Management	Various	Will process all stages of criminal case actions, from docketing in Criminal Court to final disposition in Supreme Court. Will produce an extensive array of operational and administrative reports. Will transmit data to DCJS for posting on rap sheets. Will provide a cashiering function, an interface with Family Court for Juveniles, Drug Treatment component, Summons court component, statewide inquiry into all court types (Criminal, Family, Civil), scanning and generating of documents. The OCA Domestic Violence Registry is incorporated into UCMS, with an interface to NYSPIN for Orders of Protection.

Exhibit D: DataShare Technical Strategy Subcommittee Members

Name	Agency	Title
Mary Barnett	DANY	MIS Director
Costas Deligiannis	CJA	Network Administrator
Barbara Diaz	CJA	Associate Director, Information Systems
Kael Goodman	DOC/DOP	Deputy Commissioner, CIO
Michael Hayes	DoITT	Sr. Project Manager, Enterprise Application Development
Melvin Hyatte	DJJ	Director Information Systems
Tammy Jones	DJJ	CJIS Operations Manager
Marsha Kaunitz	DoITT	Director, Enterprise Application Development
David Koosis	DOP	Director of Applications Development
Eric Lee	CJC	Deputy Coordinator
Lisa Lugo	DoITT	Assistant Commissioner, Enterprise Applications
Eliel Mamousette	DANY	Deputy Director MIS, Development
Andy Nyhan	NYPD	Lieutenant, MISD
James Pelton	NYPD	Sr. Database Administrator
Bob Plikaytis	DoITT	Director Criminal Justice Information Systems
William Power	SNP	Director, Information Technology
Don Resh	CTGi/DoITT	Data Integration & Infrastructure Consultant
Robert Schlesinger	QCDA	Director, Information Services
Scott Sigal	CJC	Policy & Information Systems Analyst
Stasi Sotiriadis	KCDA	Manager, Application Development