SPECIAL STUDY

Law Enforcement Information Management Study

Alison Brooks, Ph.D.

IDC OPINION

The objective of this study is to develop a common understanding of Canadian law enforcement's major investigative and operational systems (local, regional, provincial and federal levels) and to develop a common vision towards improved interoperability. To do so this study will provide:

- An overview of the central challenges and obstacles to interoperable systems and a view into realistic best practices of interoperability between policing systems
- An inventory and short description of the current major national, regional and provincial investigative and operational systems, smaller local systems in the policing community across Canada, and linkages between systems
- An assessment of the current levels of interoperability
- System-specific interoperability challenges
- A delineation of the reasons for a lack of interoperability and an assessment of perceived legal constraints
- Recommendations and next steps with respect to the overall state of system interoperability

October 2014, IDC #CAN11W

TABLE OF CONTENTS

TABLE OF CONTENTS — Continued

TABLE OF CONTENTS — Continued

IN THIS STUDY

Methodology

From February to August 2014, IDC conducted executive interviews with 39 of the 205 law enforcement organizations across Canada to establish a baseline understanding of major operational and investigative systems currently in use. The intent was to understand what systems organizations had in place, what systems were interconnected, and which systems needed to be connected to maximize information sharing. Interviewees were selected given their existing system knowledge, understanding of the information management challenges in policing, and geographical location as we sought to obtain an understanding of systems in place across the country. An additional five interviews were conducted to assess legal and privacy constraints to information sharing – real or perceived.

Each province is represented in the study, as are the Ontario Provincial Police (OPP), the Newfoundland Conservatory, and the Royal Canadian Mounted Police (RCMP); the Sûreté du Québec declined to participate, feeling that it would need to disclose sensitive information.

Each organization provided detailed information about the type of major operational and investigative systems in use. For each system, interviewees provided insight into the types of information collected, the entry point of the data, access and authorization, external and internal interfaces, NIEM compliance, and the internal and external organizations with which information is shared. Additionally, interviewees provided opinions on whether each system should be interconnected, and on broader interoperability gaps.

A number of areas fall outside the scope of this report, including covert systems, external systems used by law enforcement but not controlled by them (e.g., court systems, correctional systems), private sector systems, and administrative systems. Additionally, the report does not specifically address the fundamental infrastructure on which these systems operate, such as networks and operating systems.

The project team would like to profoundly thank the following organizations and individuals: the participants in this study for their time and insights; CITIG for its leadership in identifying the need for this study; the CACP ICT Committee for its leadership in supporting the proposal and ensuring that the CACP Board of Directors was briefed, and for endorsing the study, and; the Centre for Security Studies for its support and leadership in providing both the funding and capacity to move issues such as this forward through applied research.

EXECUTIVE SUMMARY

Vastly different provincial technology investments, siloed and proprietary systems, lacking interfaces and standards, a lack of a national leadership, shifting operational paradigms in policing, resource constraints, and technology limitations were cited as the key impediments to system interoperability. The sections below delve into these areas in greater depth and detail, but all of these impediments stem from siloed information systems at various levels of government.

Study participants stressed the need for an integrated and comprehensive regional/national information management ecosystem in which entity information is consolidated and shared instantly, securely, and seamlessly. Crime is increasingly mobile and does not abide by organizational, geographical or jurisdictional boundaries.

Vast differences in technology adoption occur within and between provinces and cities; with certain regions still entirely paper-based or technologically under-invested, there are vast gaps in information transfer and unnecessary delays from one system to the next.

Siloes created by proprietary systems (whether pertaining to CAD, RMS, Arrests and Bookings, BI and the need for one to draw information from another) are problematic for law enforcement, and the cause of much of the duplicate and triplicate entry of data. Creating interfaces to connect these systems is inefficient and costly. To cite but one example, proprietary systems in the digital fingerprinting space necessitate the creation of interfaces to eliminate double entry of tombstone data that already exists in law enforcement RMS systems.

System incompatibility between proprietary databases means that it is difficult, slow, and expensive to share information between systems. Standards are necessary to make systems vendor-agnostic. The use of common metadata standards allows data to be exchanged between systems without it having to be re-entered into the receiving system.

NIEM has been identified and endorsed in the CISC and via CACP for use in Canada. However, until law enforcement agencies start leveraging the tool and making it mandatory for all ICT procurements – where appropriate – the needle will not move forward.

Fundamentally, a paradigmatic shift is occurring in law enforcement globally as organizations need to shift from an operational culture based on a "need to know" basis to one based on a "need to share". Law enforcement organizations have been historically culturally reticent to share information generally, but also because of perceived privacy and legal concerns, feeling particularly guarded about sharing information pertaining to youth.

Technological obsolescence is prohibiting information sharing, particularly as it relates to PIP and CPIC. PIP was, and is, a major step forward in law enforcement information management in Canada. Prior to PIP, there was in fact no way to conduct even limited queries. While enhanced capabilities are necessary, PIP is indeed critical to operations. However, while most of Canada's 205 law enforcement organizations connect to PIP, it is currently underutilized because planned upgrades and enhancements have not been implemented.

Lacking system interoperability in fact costs law enforcement huge amounts of time and resources at a time when the financial sustainability of policing has become a mounting concern in Canada. Study participants noted that the only way a nationally or regionally integrated RMS system, or PIP 2.0, could be delivered economically, in conjunction with the quickly changing technological terrain noted above, would be through a dedicated private cloud for policing.

There are mounting pressures stemming from the consumerization of IT. With more than 70% of the Canadian population currently equipped with smartphones, the evidentiary process in all stages of a criminal investigation has changed dramatically. For Canadian law enforcement, digital evidence management (the collection, storage, analysis, and sharing of criminal information) is a *Big Data* dilemma.

A key impediment to system interoperability, and a mammoth waste of law enforcement resources, is the lack of system integration with the provincial Crowns and the judiciary. Although electronic disclosure is operational in some jurisdictions, system interoperability across the justice system simply does not currently exist and as a result there is a disincentive to adopt newer technologies. As noted above, law enforcement organizations need to integrate an increasingly diverse set of evidentiary formats (paper, video, photo, audio, etc.), attaching each piece to one investigative file number. However, more often than not, crown prosecutors' offices are ill-equipped to receive digital evidence.

As part of the LEIM study, IDC investigated the privacy and legislative landscape to better understand the boundaries, frameworks and barriers (both real and perceived) to information sharing. While this can be a very nuanced and complicated discussion, there are essentially two central dimensions relevant to the current discussion: the first is understanding the parameters of information sharing among other law enforcement organizations; the second is understanding what information police organizations can or should share with other ancillary organizations like social services, health, corrections, and education, and how they should do so.

With regards to the first area of inquiry, all of the subject matter experts interviewed for this study felt that there was little to no issue with law enforcement organizations sharing information with other police organizations in the course of an investigation. Interviewees cautioned that the law enforcement organization in question needed to have the authority to request a given piece of information, and against information-sharing where a given law enforcement organization does not have a mandate to request certain information. The need to share information among law enforcement is recognized in federal, provincial and municipal privacy legislation, and by the various privacy commissioners who enforce it.

The second dimension to information sharing pertains to multisectoral or multiagency information sharing. This has become a matter of interest recently as law enforcement, and community safety stakeholders broadly speaking, have come to recognize that community safety should not be owned solely by the police; multiagency involvement is not only necessary, but far more effective in terms of keeping at-risk people out of the system.

Historically, however, health, social services, education, and so on, have operated in isolation from one another, trying to protect the sensitive case information falling under each agency's mandate. Community safety stakeholders feel unequivocally that siloed information systems cause harm by keeping isolated agencies uninformed and only partially cognizant of the total story; early intervention

is both ineffective and nearly impossible. Police in particular feel overwhelmed by the resources they have at their disposal, and the number of calls for service that would likely be handled better by experts in adjacent areas of expertise. When people conceptualize community safety they typically think of it as the domain of police work but it is comprised of, and needs to be addressed by, a much broader group of stakeholders beyond police and corrections, including healthcare, education, social services, housing, and the municipality in question. Many of the cases that today fall into the wheelhouse of law enforcement likely shouldn't, or at least should be handled in partnership.

The Government of Saskatchewan has strategically researched and deployed an information sharing model referred to as the "HUB model" which has since been ported over successfully into Ontario under the term "Situation Tables." In standing up their multiagency systems, Saskatchewan and Ontario have conducted far-reaching reviews of their province's privacy legislation to determine how best to proceed while working with the original intent and spirit of the privacy laws. Stakeholders in Saskatchewan's HUB project reviewed all applicable legislation from all three jurisdictions, including FIPPA, PIPEDA, HIPAA, and the Child Services Act. Subject matter experts in both provinces stated that while there are certainly privacy provisions which instruct where one is unable to share information, there are also explicit instructions about when there is in fact an obligation to share as it is in the interest of the betterment of the individual.

While we are distinctly *not* proposing two-tiers of recommendations, the following are considered must-haves in the short term (being mindful that the full set is detailed at the end of this document):

RECOMMENDATIONS

Create a National Strategy

- Canadian police agencies need a national law enforcement information management strategy and roadmap.
- Law enforcement needs to stop thinking parochially, and more as provincial/regional/national enterprises.
- Research the possibility of creating a national public safety cloud.

PIP 2.0/PRP

- While PIP and CPIC provide some of the information officers need for investigations, and while there are regional pockets of integrated systems such as the OPTIC group in Ontario and BC's PRIME system, there is a need to further integrate key common data systems such as CAD, RMS, MCM and bookings systems nationally.
- PIP 2.0/PRP needs to be able to query on all RMS systems at the granular level ("tattoo on right shoulder").
- PIP should be connected with provincial driver's license databases, drawing on driver's license pictures, and consolidated with national mugshot database.

Standards/Interfaces

- CACP and its partners should strongly encourage the use of standards and NIEM-based systems to promote interoperability of existing system investments.
- Law enforcement organizations need to embed standards-based solutions into their requirements in procurements.

Mugshots

- Mugshots need to be centralized and published to the PIP 2.0/PRP. If arrest/booking/mugshot and evidence systems feed into the RMS then only the RMS would need to be interoperable. Doing so would benefit court disclosure, reduce data entry, aid data consistency, negate jurisdictional barriers and lead to more timely investigation and response.

MCM

- Explore the feasibility of connecting MCM solutions between provinces (PowerCase in Ontario, PRIME) and to national MCM systems (E&R3 and PIP 2.0/PRP).

RMS

- RMS systems need to be connected to all municipal, provincial, and federal intelligence systems, PIP 2.0, provincial justice systems, provincial transportation systems to access photos, and other regionally and nationally RMS systems. This would result in increased situational awareness, better patrol deployment, integration with provincial justice systems, predictive policing, and the consolidation of disparate information sources, and create cost savings by eliminating duplicate data entry.

CAD

- CAD systems should be connected to other emergency services (fire and EMS), provincial transportation photo databases, data warehouses and the provincial courts.

BI

- BI systems need to be connected at minimum to regional RMS systems to reduce data entry, and provide better, more complete information and enhanced situational awareness.

Digital Evidence Management/ Business Intelligence

- Law enforcement BI tools and data should be leveraged internally with other departments in the same municipality; municipal data sources could be fed into the law enforcement BI.
- Digital evidence management systems should be shared regionally/nationally, functioning as one-stop-information-shopping marts.
- Dispositions from court should come back digitally into the RMS.

SITUATION OVERVIEW

Introduction

The objective of this study is to develop a common understanding of the law enforcement major investigative and operational systems in Canada (local, regional, provincial and federal levels) and to develop a common vision towards improved interoperability. To do so this study will provide:

- An overview of the central challenges and obstacles to interoperable systems and a view into realistic best practices of interoperability between policing systems
- An inventory and short description of the current major national, regional and provincial investigative and operational systems, smaller local systems in the policing community across Canada, and linkages between systems
- An assessment of the current levels of interoperability
- System-specific interoperability challenges
- A delineation of the reasons for a lack of interoperability and an assessment of perceived legal constraints
- Recommendations and next steps with respect to the overall state of system interoperability

BACKGROUND AND A CASE FOR ACTION

The Communications Interoperability Strategy (CIST) for Canada defines interoperability as "the ability of emergency personnel to communicate between jurisdictions, disciplines, and levels of government, using a variety of systems, as needed and as authorized." [1] Law enforcement organizations must operate through multiple information "filters" such as privacy parameters and secrecy levels. By ensuring that law enforcement organizations support the CIST and the definition of interoperability, including "as authorized" stakeholders support an already existing and fairly well-known document and principle.

The burning platform driving change in policing is the consumerization of IT. With more than 70% of the Canadian population currently equipped with smartphones, the evidentiary process in all stages of a criminal investigation has changed dramatically. For Canadian law enforcement, digital evidence management (the collection, storage, analysis and sharing of criminal information) is a *Big Data* dilemma.

The Volume, Variety, Velocity and Value of Digital Evidence

Information transfer is being stymied by the volume, variety, velocity and value of information being processed. The **volume** of data coming into the evidentiary process is unwieldy. The accessibility of new data from additional sources like home security systems and body-worn cameras, the volume of new data, and the storage requirements that result, are radically changing the management of digital evidence. Law enforcement organizations are also collecting, storing and accessing far broader **variety** of evidentiary formats – paper files and notes, video, photo, audio, analytic databases, GPS

[1] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx

information, all of which need to be collated into one integrated file throughout each stage of an investigation. The **velocity** with which this is occurring is also a key challenge for law enforcement. Finally law enforcement organizations are trying to derive **value**, to work smarter, to embed evidence-based decision-making from the information contained in these proverbial siloed haystacks. Law enforcement's financial challenges have been the subject of a recent federal report, and some of it is directly attributable to mounting pressures stemming from the consumerization of IT.

Study participants stressed the need for an integrated and comprehensive regional/national information management ecosystem in which entity information is consolidated and shared instantly, securely, and seamlessly. Given that crime is increasingly mobile and does not abide by organizational, geographical or jurisdictional boundaries, the following challenges must be surmounted if the flow of information between law enforcement agencies is to be similarly fluid.

The following factors were cited as key impediments to system interoperability:

- Vastly different provincial technology investments
- Shifting operational paradigms in policing from a culture of 'need to know' to a 'need to share'
- Obsolete technical systems
- Siloed and proprietary systems
- Lack of interfaces and standards
- An historical lack of national leadership
- Resource constraints
- Difficulties interconnecting with provincial justice systems
- The absence of a Master Name Index (MNI)

The sections below delve into these areas in greater depth and detail, but all of them stem from or contribute to siloed information systems at various levels of government.

Vast Differences in Technology Investments

Vast differences in technology adoption occur within and between provinces and cities. With certain regions still entirely paper-based or technologically under-invested, there are vast gaps in information transfer, unnecessary delays from one system to the next. For example, of the 35 law enforcement organizations in Quebec, only 3 leverage RMS systems; the rest remain paper-based.

Shifting Operational Paradigms in Policing

There is a paradigmatic shift occurring in law enforcement globally as organizations need to shift from an operational culture based on a 'need to know' to a 'need to share'. Law enforcement organizations have been historically culturally reticent to share information generally, but also because of perceived privacy and legal concerns, feeling particularly guarded about sharing information pertaining to youth. There is a difference between connecting and sharing; a lot of law enforcement organizations are able to query but a lesser number post information.

Technical Obsolescence of Critical Systems

Obsolete systems are being maintained for a number of reasons, including lack of funding, organizational culture, internal dependencies, a lack of resources and a lack of national leadership. Law enforcement organizations feel that technological obsolescence is prohibiting information sharing, particularly as it relates to PIP and CPIC. PIP was, and is, a major step forward in law enforcement information management in Canada. Prior to PIP, there was in fact no way to conduct even limited queries. While enhanced capabilities are necessary, PIP is indeed critical to operations. However, while most of Canada's 205 law enforcement organizations in Canada connect to PIP, it is underutilized as many stakeholders feel that the information is:

- Limited in scope, functionality and query capability
- Inconsistently entered from one organization to the next
- Shallow or frequently incomplete
- Unreliable in terms of data quality due to reporting inconsistencies

Inconsistency, shallow data and unreliability are not so much technology issues, but rather expensive auditing issues and a challenge to policing.

While PIP is fully able to supply detailed occurrence information by clicking on a hot link on the screen, access for some users may be denied as a result of a security policy relating to 2 Factor Authentication, which would make PIP appear unable to provide detailed information.

It is important to recognize that the constrained search functionality was the intended original scope of PIP, recognizing that enhancements and iteration would be necessary; however, these enhancements have not occurred.

Proprietary Systems

Siloes created by proprietary systems (whether it pertains to CAD, RMS, Arrests and Bookings, BI and the need for one to draw information from another) are problematic for law enforcement, which often leads to duplicate and triplicate data entry. Proprietary software or closed source software is computer software licensed under exclusive legal right of the copyright holder with the intent that the licensee is given the right to use the software only under certain conditions, and restricted from other uses, such as modification, sharing, studying, redistribution, or reverse engineering. [2]

Usually the source code of proprietary software is not made available.

Creating interfaces between systems is inefficient and costly. One example of proprietary systems is in the digital fingerprinting space, where organizations need to create interfaces to eliminate double entry of tombstone data that already exists in law enforcement RMS systems. System incompatibility between proprietary systems means it is difficult, slow and expensive to share information.

[2] http://en.wikipedia.org/wiki/Proprietary_software#cite_note-1
http://en.wikipedia.org/wiki/Proprietary_software#cite_note-linfo-2

Lack of Standards

Standards are necessary to make systems vendor agnostic. Use of common standards allows data to be exchanged between systems without it having to be re-entered into the receiving system. RMS and CAD vendors like Niche, Intergraph, and Versaterm all offer proprietary, solution-specific systems. NIEM has been identified and endorsed in the CISC and via CACP for use in Canada. However, until law enforcement agencies start leveraging the tool and making it mandatory for all ICT procurements – where appropriate – the needle will not move forward.

Standards-based solutions allow law enforcement organizations nationally to leverage economies of scale, creating cost savings from the lack of double-entry and search time. Lastly, standards help to mitigate project risk; participants from Alberta noted that had the API3 project in Alberta been built on standards-based systems, the project might have been saved.

Lack of National Leadership

The lack of national leadership was noted frequently as a very real strategic and operational gap with participants feeling that the collective publication of data to a shared environment would allow organizations to operate much better, and stressed the need for a national roadmap for organizations to follow.

Financial Instability

According our study participants, lacking system interoperability costs law enforcement quantum amounts of time and resources at a time when the financial sustainability of policing has become a mounting concern in Canada. According to the recent Canadian federal government report on the economics of policing: "During a time of fiscal restraint and enhanced public expectations, governments and police services must find more efficient and effective methods to sustain current levels of policing services to ensure public safety." [3]

Study participants noted that the only way a nationally or regionally integrated RMS system, or PIP 2.0, could be delivered economically, in conjunction with the quickly changing technological terrain noted earlier, would be through a dedicated private cloud for policing. The February 2014 CACP ICT workshop in Vancouver endorsed the need to research creating a national cloud for policing and public safety.

System Interoperability Across the Justice Continuum (eDisclosure and DEMS)

A key impediment to system interoperability noted by participants was the mammoth waste of law enforcement resources trying to transfer information with the provincial Crowns and the judiciary. Although electronic disclosure is operational in some jurisdictions, system interoperability across the justice system simply does not currently exist and as a result there is a disincentive to adopt newer technologies. As noted above, law enforcement organizations need to integrate an increasingly diverse set of evidentiary formats (paper, video, photo, audio, etc), attaching each piece to one investigative file number. More often than not, crown prosecutor's offices are ill-equipped to receive digital evidence.

[3] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/smmt-cnmcs-plcng-2013/index-eng.aspx#_Toc350350734

Master Name Index (MNI)

The creation of a local MNI that is accurate and complete is an on-going challenge for police services and law enforcement in general. Individuals do not have unique name / sex / Date of Birth (DOB) combination and as a result it is often difficult to distinguish one person from another. For example, someone may indicate that the person who committed the assault is John Smith, but they have no idea what his DOB may be. Added to this is the fact that reporting conditions tend to produce incomplete records entries. Often the same person is represented a number of times in the MNI due to various DOBs or spellings of the name. An accurate and complete MNI would be an invaluable asset to policing, but remains elusive. Where charges involved, fingerprints provide a distinguishable uniqueness but charges only occur in some 10% of occurrences. An accurate, consolidated MNI is an even bigger challenge nationally.

SYSTEM INVENTORY

As noted above, a central purpose of this study is to provide insight into what major operational and investigative systems are currently in place in Canadian law enforcement. While the study was open to input on *all* major operational and investigative systems, we specifically probed each organization from the following list of systems as determined by the project team:

- Computer aided dispatch (CAD)
- Records management systems (RMS)
- Major case management (MCM)
- Business intelligence (BI)
- Criminal justice information management systems (CJIMs)
- Arrest and bookings
- Digital evidence management
- Jail and cell management
- Mobile reporting solutions
- Citizen portals

Most law enforcement organizations in Canada leverage the full gamut of systems noted above. However, some of the smaller municipal forces tend simply to field basic CAD and RMS systems.

The study inventoried 367 system entries from the 39 organizations interviewed. Excluding duplicate entries, those 367 can be distilled into 144 distinct separate systems (excluding modules of larger systems). On average, each organization we spoke with operates approximately 10 different systems. It merits noting that the number of CAD systems is likely lower due to the consolidation of dispatch services.

The following table summarizes the number of systems by system-type:

System Type	Number
RMS (records management)	76
Arrest and Booking System	46
BI (business intelligence)	45
CAD (computer aided dispatch)	37
Other	36
Jail/cell management system	26
MCM (major case management systems)	25
Mobile Reporting	25
Criminal Justice and Information Management Systems	22
Digital Evidence Management system	16
Scheduling	8
Citizen portal / Database	2
eTicketing/Licence plate reading	2
Content Management	1
Total	367

Representation by province is roughly in keeping with provincial population levels. The following table is a summary of the percentage of systems inventoried by province, as contrasted with the population percentage for each province. While we did not align quotas by province, we did seek to ensure relatively equal representation. New Brunswick and Nova Scotia appear to be slightly oversampled, while Quebec appears under-sampled. The Quebec skew is not troubling given that we interviewed 100% of the local police forces with operational RMS and CAD systems.

Province	% of systems inventoried	% Population
AB	10%	11
BC	12%	13
MB	4%	3.6
NB	8%	2.2
NFLD	1%	1.5
NS	5%	2.8
ON	45%	38
PEI	4%	0.4
PQ	8%	24
SK	3%	3.1

The following sections provide an overview of the major operational and investigative systems and consortiums, including where the data stems from, access, whether the system is shared and the extent to which it interconnects to other systems. The section begins with larger national and regional systems in use in Canada: PIP, CPIC, PRIME, OPTIC, PROS, etc., followed by the primarily local (CAD, RMS, BI, Arrests and Bookings, Jail and Cell Management, etc), and, lastly the provincial systems (MCM, CJIM).

LARGE NATIONAL AND PROVINCIAL SYSTEMS

Police Information Portal

Managed by the RCMP, the Police Information Portal (PIP) is a searchable national index of police agency RMS systems that provides a hyperlink back to each police agency's Record Management Systems to read the original file. It should be made clear that PIP is not a true data source but is rather an interface with source databases to collect and share information.

On average, PIP processes one million queries per month; over the last year, PIP processed more than 25 million maintenance transactions. The PIP database contains 35 million person records and 14 million vehicle records. Access to the database is available to all sworn and civilian law enforcement as role dictates, and is used by approximately 90%-95% of all law enforcement agencies in Canada. PIP interfaces with most law enforcement agencies' RMSs, PROS, PSP, SAMS, CIIDS, and PRIME in BC. Connections to other systems occur via interface. By way of clarification, there is a difference between query capability and publishing; almost all law enforcement organizations query but a much smaller number publish – which is an issue.

In July of 2014, the RCMP issued an RFI for the next generation PIP, referred to as the Police Records Portal (PRP). According to the RFI, "as crime becomes more global, the need to continue sharing public safety information nationally remains crucial. Efficient and effective information sharing among public safety agencies, including police, remains a key element in ensuring public security."

Canadian Police Information Centre

The Canadian Police Information Centre (CPIC) provides investigative, identification, intelligence and ancillary data on persons, vehicles, marine, property, driver's licenses, warrants, criminal records, fingerprints, firearms registration, surveillance, inmates, and the Automated Canada United States Police Information Exchange System (*ACUPIES*). It can also act as a real-time officer safety system. Like many other systems, CPIC needs to be updated to meet current requirements. For example, a photo of a missing person cannot be stored on CPIC today. In 2011 CPIC held more than 10 million records and processed more than 200 million queries through 40,000 access points. More recent statistics from 2013 show CPIC processing 684,000 transactions per day, 50,000 transactions at peak hour, in less than 0.25 seconds response time at peak hour. The information in CPIC is an amalgamation of other RMS data automatically pushed to it. CPIC is shared with other law enforcement organizations across the country, provincial motor vehicle, stolen vehicle, convictions, municipal organizations, federal government organizations like CSIS and CBSA and a number of police forces in the U.S. through NLETS (the U.S. National Law Enforcement Telecommunications System). These arrangements have come under recent scrutiny as U.S. border officials have been leveraging the CPIC information to deny citizens entry because of mental health history. Canada's national and provincial privacy commissioners have conducted inquiries and made recommendations to address these matters.

Canadian Criminal Real Time Identification Services/Real-Time Identification Project

The Canadian Criminal Real Time Identification Services (CCRTIS) mandate is supported by a number of initiatives, including both criminal and civilian screening services, the most pertinent of which are the Criminal Records Information Management Services (CRIMS), Real-Time Identification (RTID) and LiveScan, Civil Fingerprint Screening Services (CFSS) and Automated Fingerprint Identification System (AFIS).

Real-Time Identification Project

Under the CCRTIS modernization initiatives, in 2010 the RCMP implemented a policy directive to nationally migrate to digital fingerprints by 2014. LiveScan is the RTID arrests and bookings system that is replacing the old fingerprints paper forms. Inkless electronic fingerprinting is much more efficient, avoiding smudging, smearing and improper inking associated with traditional ink prints. Processing time is completed within 3 days, versus up to 120 days with rolled ink prints. The benefits of migrating to digital are delineated on the RCMP RTID web page: "Real Time Identification (RTID) is … designed to improve the efficiency of Canada's national fingerprint and criminal record repository. Outdated paper processes and legacy systems will be replaced by modern technology, re-engineered workflows and automation to support interoperability with all users of the NPS Canadian Criminal Real Time Identification Services (CCRTIS) fingerprint and criminal records services. RTID efficiencies are directly related to reducing the number of paper-based fingerprint submissions and, in turn, increasing

the number of electronic fingerprint submissions."[4] For police agencies, the central challenge to implementing RTID is cost.

RTID is an RCMP managed system that provides biometric-based criminal record verification services, which are used for both criminal justice and non-criminal justice (civil and immigration screening) purposes. The RTID system provides the technical capabilities that allow National Polices Services Agencies, government agencies, and authorized private organizations to submit queries to verify a set of fingerprints against the RCMP Criminal Record holdings.

RTID is shared in the sense that Canadian law-enforcement and public safety organizations and government departments contribute information to the system. LiveScans are also used by government agencies such as CIC, CBSA, and Transport Canada. RCMP connects the LiveScan RTID with National NIST Server (NNS); other policy agencies may connect with their local RMS.

This information is accessed by these organizations and authorized private sector organizations for the purposes of criminal record verifications. It is also accessed by international law-enforcement organizations under an appropriate Memorandum of Understanding, that takes into account Canadian legislative and privacy restrictions.

The RCMP maintains a repository that includes approximately 4.5 million criminal records – the National Repository of Criminal Records (NRCR) – relating to individuals that have been charged with or convicted of offences in accordance with federal laws. Each criminal record in the repository includes lawfully obtained fingerprints, pursuant to Canada's Identification of Criminals Act. It also holds biographic information and the associated fingerprints on behalf of Citizenship and Immigration (CIC) and the Canada Border Services Agency (CBSA) for immigration clients who apply to visit, work or migrate to Canada under the Temporary Resident or Refugee programs.

The NRCR, in addition to a number of internal back-end systems support the delivery of RTID. Most notably are: the Automated Fingerprint Identification System (AFIS), a commercial-off-the shelf (COTS) product that specializes in fingerprint matching capabilities; CPIC, the system of record for Criminal Record information, and; the Criminal Justice Information Management (CJIM) system. The AFIS component is an integral part of the RTID system and is interconnected to internally developed components of the system through a strictly defined Interface Control Specification. This allows the RCMP to replace the AFIS component as required in a seamless manner. The CPIC component is inter-connected to the RTID system via a MQ Series interface and uses the standard CPIC queries and maintenance transactions to interface with CPIC.

It also supports the Canadian immigration program by providing it with identity management services for interaction with clients throughout the immigration program.

[4] http://www.rcmp-grc.gc.ca/rtid-itr/index-eng.htm

Civilian Screenings

As noted above, public and private organizations are increasingly relying on criminal record information for various civil and/or administrative screening purposes. Under the broad context of civil or administrative screening purposes, criminal record information may be verified to ascertain an individual's suitability for various purposes, such as employment, volunteering, adoption requests, legal name changes, and eligibility for entry into Canada under various immigration programs and is now a standard and critical component in background screening. These screening measures are used for public safety and security purposes and contribute to protecting organizations from possible criminal activity and insider threats, such as unauthorized access to financial and other critical infrastructure systems. All public and private organizations are accredited and authorized prior to having access to the information in RTID. Legislative and policy factors determine which information is releasable to these organizations. Civilian screening processes are labour intensive and some organizations believe that the police need not be the provider.

Automated Criminal Intelligence Information System

The Automated Criminal Intelligence Information System (ACIIS) database is populated by analysts and various enforcement agencies and functions as a national intelligence repository for the use of all Criminal Intelligence Service Canada members in Canada. Member agencies cooperate with each other in the collection, collation, evaluation, analysis and dissemination of criminal intelligence by contributing to ACIIS. It is managed by and shared with RCMP units, as well as being shared with all Criminal Intelligence Service Canada members in Canada.

Police Records Information Management Environment

In 2003 the province of BC mandated integration of all of the provinces' CAD, RMS, MCM and MDT systems into one province-wide system called the Police Records Information Management Environment (PRIME). This Versaterm-based centralized system, connects every municipal police department and RCMP detachment throughout the province, providing law enforcement with instant access to information via three mirrored provincial systems. The system is owned and managed by PRIME Corporation, a subsidiary of E-Comm. Of all the provinces we studied, BC is the most integrated and interoperable from a systems perspective.

The PRIME RMS is accessible by all 9,000 sworn law enforcement members in BC, plus law enforcement organizations with broader access to PIP, to which PRIME interconnects via interface. The RMS also connects to PIP, and to JUSTIN, the provincial CJIMS. The PRIME system has a number of system modules embedded within it, such as Arrest and Bookings, Jail and Cell Management. The Arrest and Bookings module interfaces with iBook; the Jail and Cell module does not connect to other systems. The Evidence continuity module connects via interface to PIP.

PRIME has significantly reduced the burden of duplicate data entry, increased data quality, and bolstered the system's analytical capacities. Records created via MDT are instantly available to officers back at the detachment. The RCMP and PRIME have been testing a link from IntelliBook (iBook) to allow agencies to capture digital fingerprints and photographs of persons accused, and submit the fingerprints to the National Real Time Identification (RTID) records system. However, similar to comments made below about the OPTIC collective in Ontario, the magnitude of the system means that changes are slower to make in PRIME.

Police Reporting and Occurrence System

Based on Niche technology, the Police Reporting and Occurrence System (PROS) is now owned and managed by Bell Canada. PROS is a pan-Canadian RMS system for the RCMP and 23 police partner organizations, with a combined 19,000 daily active users, with 13 different interfaces to other systems. According to a 2011 audit of selected RCMP databases, PROS is a "complete occurrence and records management system containing information on individuals who have come into contact with police, either as suspects, victims, witnesses or offenders, from initial occurrence to final disposition…. About 1.6 million occurrence files are processed per year." (2011 Audit of Selected RCMP Operational Databases). PROS interconnects with a plethora of other systems: PIP, FIP, MIS, SAMS, PADS (Pardons), Historical Copy stats database, CPIC, IQT, and PAT.

Ontario Police Technology Information Cooperative

The Ontario Police Technology Information Cooperative (OPTIC) links data from over 8,000 police officers across 43 Ontario municipal police forces, and the OPP, on to a single Niche RMS installation, reportedly making it one of the largest data sharing initiatives in North America. The Niche OPTIC cooperative interconnects to both CPIC and the Province's Major Case Management system, PowerCase.

Centre de Reseignement des Policiers du Québec

Akin to "PIP," the Centre de Reseignement des Policiers du Québec (CRPQ) is a provincially shared system in Quebec that imports RMS data twice daily. The system accesses additional provincial data repositories (License bureau, other police agencies occurrences, etc.). CRPQ interfaces with CPIC.

Miscellaneous National Systems and Registries

As each national system is upgraded, the RCMP has created a web-based portal to access each system individually. Usually, interfaces are looked at in secondary or subsequent phases. For agencies that rely on their RMS systems this seems to be a backward approach.

Evidence & Reporting 3

Evidence & Reporting 3 (E&R3) is the only nationally recognized MCM system that tracks and links large amounts of investigation-related information. Given the sensitive nature of the information, inputs to the system and access to the data is restricted to case-specific investigators. While it is RCMP-wide, it is not centralized; there are many instances of it across the country that are not interconnected. There is a project currently underway to define the business case options to replace the E&R3 MCM system. E&R3 is also used by certain smaller law enforcement organizations as their MCM tool.

Violent Crime Linkage System

Created in the early 1990's, the Violent Crime Linkage System (ViCLAS) is an automated case linkage system for major case crimes (homicide, sexual assault, missing persons, etc.) with analysis centres in all provinces (except PEI). Case information is submitted to the system by investigating officers; the system is accessible only by select members in investigations. The system is managed by the RCMP and the OPP and is accessible broadly to other law enforcement organizations across the country.

National Sex Offender Registry

Developed and administered by the RCMP, the National Sex Offender Registry (NSOR) was established by the Sex Offender Information Registration Act (SOIRA), proclaimed as law on December 15, 2004. It is a web-based application available to all accredited Canadian and International law enforcement agencies. NSOR and the Ontario Sex Offender Registry (OSOR) recently merged.

Internet Child Exploitation Unit

Internet Child Exploitation (ICE) is child exploitation tracking software developed by Microsoft Canada, the RCMP and Toronto Police Service. Study participants could not specify whether the system interconnected with other systems.

PRIMARILY LOCAL SYSTEMS

Computer-Aided-Dispatch

Computer-Aided Dispatch (CAD) systems receive calls for service and dispatch emergency service organizations accordingly. CADs communicate incident information to the MDTs in the case of law enforcement and push their information directly to the organization's RMS via interface. CAD systems tend only to interconnect with the internal RMS. All but one of the law enforcement organizations we interviewed for this study had implemented a CAD system. The CAD specifically is accessed by call takers, dispatchers and supervisors. CAD systems in Canada are essentially split between two vendors – Intergraph and Versaterm – with a smattering of organizations that have implemented custom solutions.

CAD systems are primarily managed locally; however, the RCMP maintains its own CAD and requires some further details given its size and importance. As part of its modernization initiative, the RCMP CAD has been modernized considerably by Bell, and will be consolidated from eight dispatch centres into one based out of Ottawa. The RCMP CAD interconnects with a plethora of other systems including: CPIC, CPIC MF, Ontario and BC PARIS, PROS (add only), PIP (query only), OnPatrol, Division radio systems and E911.

Records Management Systems

Law enforcement organizations use Records Management Systems (RMS) to integrate incident-based information on general occurrences into a cohesive database. The RMS data interfaces with the call for service information from the CAD, and other data sources like mugshots and fingerprints from arrest and bookings systems. Generally, all sworn officers and civilians have access to the RMS. RMS data interfaces with PIP, although in varying degrees of detail and consistency.

Of the 39 organizations we interviewed there is a fairly even split between two RMS vendors – Versaterm and Niche. This seems to align with broader findings from across the country. According to the Police Records Portal RFI, in Canada "RMS solutions vary from custom/in-house developed applications to commercial off-the-shelf (COTS) solutions. Outside of the province of Quebec, the

RMS market is divided fairly evenly between the Versaterm/Versadex RMS and the Niche RMS. Index Generale is the primary RMS used in Quebec." (POLICE RECORDS PORTAL – RFI, GETS Ref. No. PW-$$XL-119-27785).

Arrest and Bookings

Arrests and Bookings systems process an array of inputs including fingerprints, mugshots, charges, and charge dispositions, physical descriptors of the accused including marks, scars and tattoos and, in some cases, digital recordings and video of intake interviews. A large number of the organizations we spoke with leverage arrest and bookings as a module within their RMS systems; the study catalogued an additional 20 arrest and bookings systems.

Arrest and bookings systems typically connect to the municipal law enforcement RMS and, federally, to CCRTIS/RTID. Mugshots are most frequently posted to the local RMS and from there to PIP but this is not universal practice. Fingerprints, conversely, are universally pushed to the RCMP.

The most frequently leveraged Arrests and Bookings systems were, alphabetically, Accellium, Cogent, For the Record, IntelliBook (iBook), IntelliScreen (for civilian printing), and LiveScan/RTID.

Business Intelligence

BI systems extract data from other systems and administrative files, particularly CAD, RMS, MCM systems and non-localized statistics databases, with some organizations also leveraging HR and finance information. The information is consolidated into reporting, analysis, dashboards, scorecarding and predictive analytics capabilities. Most of the law enforcement organizations we interviewed had some sort of business intelligence system from vendors like Cognos, eCrime, ESRI, GR (Gestion du renseignement), IBM - i2, Informatica, Innovative Data, Omega Group and Palantir. Organizations commonly have multiple BI systems.

Some systems, like Sonar, are designed for niche purposes like analyzing data generated through social media sites. Veteran suppliers Cognos/IBM and ESRI were the most prevalent systems used; Tableau and Palantir stood out as relatively new, well-received systems. BI systems generally are not shared or interconnected with other law enforcement organizations locally, provincially, regionally or nationally.

BI and the RCMP

The RCMP runs a single centralized instance of Cognos' BI solution in their Business Intelligence Centres currently in Vancouver and Ottawa but soon to be established in other large metropolitan areas. Data sets include finance (contract police reporting, fleet, real estate), HR, firearms (primarily CFIS), operational reports (E Division only – mostly related to calls for service), performance management, forensic science and identification services (RTID, LIMS). It does not interconnect with other systems, nor is it shared.

The RCMP is also currently building a new enterprise data warehouse internally connecting a copy of number of large information databases like PROS, PRIME, E&R3, AFIS, and others. The data

warehouse will integrate, standardize and secure the information, and will run Google-like search on top of it. However, it is to be leveraged internally only by the RCMP and is not intended to connect to other RMS's.

Mobile Reporting

Mobile Reporting (MR) systems are leveraged via the officer's in-car mobile data terminals (MDTs), and, for some smaller enterprising forces, via smartphones (see below). Study participants also consider civilian incident reporting to fall into the mobile reporting suite of major systems.

MR allows law enforcement to access CAD and RMS systems remotely, accessing general occurrences, street checks, tickets, motor vehicle collision reports, and so on, and to query other federal and provincial databases like CPIC, PIP, Motor Vehicle interface, and Crimes Management Systems. MDTs also provide real-time information about active users, active units and active incidents.

Mobile reporting solutions tend not to be shared outside of the local organization, though they are typically interconnected to the RMS, CAD, and the typical federal and provincial databases noted above. Study participants did not see value in making the MRE more interoperable, with the exception of Chatham-Kent, who felt that connecting the mobile solutions more broadly would provide officers with a much richer mobile environment.

Chatham-Kent is currently running a mobile reporting Blackberry pilot for Ontario, seeking to keep officers mobile, by empowering them to do everything they would otherwise do from their car. The system is being piloted by all 170 Chatham-Kent police officers. Having essentially missed the implementation window for MDTs, Chatham-Kent was able to move straight to mobile. The pilot connects to their RMS, PIP, CPIC, and MTO ISS. The BlackBerry linkage to the RMS and CAD was built by Mobile Innovations out of Waterloo.

Digital Evidence Management Systems

The staggering challenges created by proliferating digital evidence mean that Digital Evidence Management (DEM) systems are becoming increasingly vital operational and investigative systems. DEM systems integrate all digital evidence and/or information with the main purpose of expediting evidence management in general, and minimizing the amount of time and effort law enforcement must put into the disclosure process.

While Canadian law enforcement is fairly new to this market a quick, but non-exhaustive survey of the DEM systems landscape reveals a number of key vendors in this marketplace, including Otec Solutions, Reveal Media, Evidence.com, MediaSolv, CaseWorks, VeriPic, Rimage and Enara. While many of our interviewees leveraged modules from their existing RMS vendors, others noted Dell eCRIMES, MediaSolv, Panasonic Arbitrator, PRIME, and For the Record as DEM systems in use in their organizations.

Two organizations are leveraging custom systems to create efficiencies pertaining to the burden of court disclosure: Edmonton and Chatham-Kent. Durham is leveraging a DEM for video forensics.

Edmonton

The City of Edmonton and Alberta Crown Prosecution Services (ACPS) are implementing a project with OpenText and Accellion to digitize their disclosure process, gaining efficiencies for both police and the courts. Accellion is in fact an Enterprise File Synchronization and Share solution, in essence a secure drop box file transfer. In combination with OpenText the files are transferred with an electronic signatures application within a secure electronic process. Digitization of the disclosure process is not only a far more efficient use of police resources, it also saved two tonnes of scanned documentation in the courts. Once the disclosure process went digital, guilty pleas increased sizably as defence attorneys could no longer argue that their client's identity could not be determined from a rescanned, indecipherable mugshot.

Chatham Kent "eBrief Project"

Chatham-Kent's eBrief project, leveraging Adobe, Xerox, and Dragon Dictation, is seeking to convert all existing paper briefs, disclosure documents, and court documents to digital file format, delivered to all parties digitally as a single secure, searchable, traceable/auditable PDF. The file includes all digital data including lengthy videotaped interviews, 911 audio files, mugshots, cell block video, and bookings.

Durham leverages Dell eCrimes to extract photographic and videographic child pornography evidence from seized hard drives and cell phones. It was noted that a provincially available solution, connected to the SOR does not currently exist but would be valuable.

One of the key challenges to interconnecting DEM systems is the standardization of video formats between organizations, parts of an investigation, and in terms of archive.

Jail and Cell Management Systems

Jail and cell management systems consist primarily of surveillance systems and people/asset tracking. The former include camera and/or video for interview rooms, CCTV monitoring, and the storage and archive solutions behind it. The latter addresses the software to manage offender transfers, staff management and guard checks, and tends to be leveraged as custom modules in RMS and CAD systems. According to those interviewed for this study, the vast majority of these systems are not shared, nor do they interface with other systems, with the exception of the PRIME environment in which the systems are shared with the other law enforcement agencies that are part of PRIME and connect directly to the PRIME RMS. Study participants felt that there would be time savings to connecting these systems to the RMS and to the electronic disclosure case file.

Citizen Portals

Citizen portals consist of online non-emergency incident reporting tools and internal applications that allow citizens to view geo-mapped data of crime.

Coplogic – Coplogic is a citizen portal that connects directly to the RMS once the information is vetted by an officer. The system allows the public to contact police about non-emergency situations such as graffiti, vandalism, and stolen property. Coplogic will handle rich media in the future.

E-Reporting – Like Coplogic, E-Reporting is a public-facing web server that allows citizens to file minor offence reports online, acting as a functional alternative to the standard call taking / dispatching / report writing business process for many (lower priority) call types.

Miscellaneous Systems and Registries (Local)

Dragon Dictation – Dragon dictation is a Siri-like voice recognition system, accessible on BlackBerry, which allows officers to verbally enter reports that are then directly entered into the RMS after the records unit has proof-read the material. Training requirements are fairly minimal with officers needing to spend two hours training the system to recognize their voice patterns and intricacies.

MAJOR PROVINCIAL SYSTEMS

Major Case Management

Ontario — PowerCase Major Case Management (MCM)

Owned and operated by the OPP, all of Ontario's municipal police services have had access to Ontario's MCM since 2002. MCM connects to all municipal and regional police force's RMS systems in Ontario and with the RCMP. Study participants felt that Ontario MCM should connect to other provincial or national MCM systems.

PRIME-BC

PRIME MCM, a subsystem of the Versaterm RMS, contains sensitive information related to organized crime investigations and is therefore limited in terms of access to investigators and records personnel from BC law enforcement and the RCMP. The PRIME MCM interfaces with JUSTIN, CPIC, and PIP.

- Saint John's New Brunswick Public Sector Case Management (SunGard) – Local MCM solution used in Saint John's NB; not connected to other systems.
- Charlottetown PEI – Major case management module within OSCIS. Does not specify interconnectedness.

Criminal Justice Solutions

Study respondents generally supplied very minimal information regarding criminal justice solutions, so this section will only briefly list and describe the systems.

CJIM – The Federal Criminal Justice Information Modernization (CJIM) project, spearheaded by the RCMP, was launched in April 2013 to allow participating police agencies to submit electronic criminal charges, substantially reducing requirements for paper charge submissions.

eJust – A select number of municipalities in Ontario use eJust as a charge management system to compile crown briefs, charge information, and court documents. eJust connects to the RMS and

IntelliBook. Some organizations have implemented the technology seamlessly, while others have experienced challenges migrating to eJust given decisions made during implementation.

ICON – ICON is a case tracking and scheduling solution used in Ontario to manage digital information about individuals, charges and docket schedules.

Réseau Justice – Quebec's court charge system containing information on charges, person information, court dates, sentences, etc.

JUSTIN – JUSTIN is the custom-built BC Provincial Government Court Data application, containing offender and court data. It is accessible to select people, and shared with the RCMP, corrections and courts. Study participants felt that JUSTIN should be shared with both Prime and PIP.

JOIN – Justice Online Information Network (JOIN) is used in Medicine Hat Alberta to manage charges, ongoing court management, and dispositions. Built by the Province, it is accessible to police, corrections, and justice, but requires better integration with the local RMS.

NS Provincial Court System (Electronic Offense Summary Tickets) – Link from digital tickets to the RMS and to the provincial justice system.

CURRENT LEVEL OF SYSTEM INTEROPERABILITY

Interoperable Systems

In the aggregate, only 36% of the system entries we catalogued were interconnected to other systems; of that subset, 40% connect internally (from a CAD system to the RMS, etc.) indicating that there is little systemic information sharing between organizations or jurisdictions.

The following table lists by system type the percentage of systems that interconnect with other systems. A few caveats need to be made. First, while 100% of citizen portals are interconnected, it is important to note that there were only two systems classified as citizen portals. Second, for somewhat obvious reasons, of all the major investigative and operations systems, RMS and CAD solutions are the most frequently interconnected, with the CAD system pushing incident information to the RMS despite frequently being from different proprietary vendors. RMS systems interconnect with the CAD, CPIC, PIP, the provincial MCM, and less frequently with other provincial databases like transportation. Outside of OPTIC and PRIME, they do not generally connect with other RMS systems, or other systems like DEM, BI or other provincial MCM systems. While mobile reporting appears highly interconnected, 70% is internally to the CAD and RMS. Study participants did not see value in making the MRE more interoperable, with the exception of one organization that felt that connecting the mobile solutions more broadly would provide officers with a much richer mobile environment. Arrest and bookings systems are interconnected locally with the RMS for mugshots and externally to CPIC for fingerprints. Business Intelligence systems are only very rarely connected with other systems. BI systems are typically built over data warehouses that contain a consolidation of files from disparate systems, so the interconnectivity is not significant factor. The more important factor is the contribution of data from various systems into the data warehouse.

System Type	% Interconnected
Citizen portal / Database	100%
CAD (computer aided dispatch)	70%
Mobile Reporting	60%
Arrest and Booking System	50%
eTicketing/License plate reading	50%
RMS (records management)	49%
Digital Evidence Management system	31%
Criminal Justice and Information Management System	23%
BI (business intelligence)	20%
MCM (major case management systems)	20%
Other	8%
Jail / cell management system	8%
Content Management	0%

Proprietary RMS and CAD Solutions Inhibiting System Interoperability

As mentioned earlier, of the 39 organizations we interviewed there is a fairly even split between two RMS vendors, Versaterm and Niche; an analysis of the CAD and RMS systems of those organizations unveiled some profound local variations and a lack of provincial and/or national integration:

- The seven police forces we spoke with in the Atlantic Provinces operated six different CAD systems; one municipal police force did not actually have a CAD system. On the RMS side, there was some amalgamation in the Atlantic provinces with PROS (the Police Reporting and Occurrence System), operated by the RCMP.
- The province of Quebec lags considerably in terms of technology implementation and as a result is highly fragmented – both within the province, and when sharing information nationally. Only three of the thirty-five police agencies in Quebec have implemented an RMS system; according to the three forces we spoke with from Quebec, the rest of the police forces in the province are still operating paper-based systems.
- Of the 15 organizations we spoke with from Ontario, including the OPP, seven are part of the OPTIC collective running Intergraph CAD and Niche RMS, seven run Versaterm for both their CAD and RMS, and one last Ontario force – Toronto – deploys a combination of both. The OPTIC collective has full visibility into each other's data, but they have no visibility into the other RMS systems run by Versaterm, frequently in adjacent municipalities.
- In the prairies, while Winnipeg and Regina both have Intergraph CADs and Niche RMS, Saskatoon has the opposite – Versaterm RMS and CAD.

- In Alberta, while Edmonton and Calgary both have Intergraph CAD systems, their RMS systems are proprietary or custom (Niche and PIMS) and do not interconnect.
- To reiterate, the province of BC was mandated to integrate all of the provinces' CAD, RMS, MCM and MDT systems into one province-wide system called PRIME. Of all the provinces we studied, BC is the most integrated and interoperable from a systems perspective.
- The RCMP itself leverages different RMS and CAD systems in different provinces across the country. In BC for example, it uses PRIME, created by Versaterm, Elsewhere it leverages the PROS system, and in Halifax District uses Versaterm provided to it by the Halifax Regional Police.

Shared Systems

The following Table lists the percentage of systems ***shared with other organizations***. Again, note the low n-value for citizen portals and that by definition they are shared externally. RMS and CAD solutions are the most frequently shared with one another. MCM solutions are typically provincial in orientation and shared accordingly. Arrest and Bookings systems are shared internally, with the RMS, and externally, nationally with CPIC. DEMs and BI solutions surprisingly tend to be isolated within one specific organization. Mobile reporting solutions tend not to be shared outside of the local organization, though they are typically interconnected to the RMS, CAD, and to federal and provincial databases like CPIC, PIP, Motor Vehicle interface, and Crimes Management Systems.

System Type	% Shared
Citizen portal / Database	50%
RMS (records management)	42%
CAD (computer aided dispatch)	38%
MCM (major case management systems)	24%
Arrest and Booking System	24%
Criminal Justice and Information Management System	23%
Digital Evidence Management system	13%
BI (business intelligence)	11%
Mobile Reporting	8%
Jail / cell management system	8%
Other	6%
eTicketing/License plate reading	0%
Scheduling	0%

SYSTEM-SPECIFIC INTEROPERABILITY CHALLENGES

PIP

As noted earlier, PIP is underleveraged as stakeholders feel that the information is limited in query ability, shallow, and inconsistently entered from one organization to the next. There seems to be inconsistency regarding how PIP is used. Some feel that they need to telephone the originating organization to receive a complete file while others feel they have unfettered and instantaneous access to the originating RMS information. This inconsistency can be attributed to three possibilities: an improperly functioning interface, a training issue, and the organizations aren't allowing the functionality to allow the query to produce the report. Upon further investigation, it appears to be the latter. While PIP is fully able to supply detailed occurrence information by clicking on a hot link on the screen, access may be denied as a result of a security policy relating to 2 Factor Authentication, which would make PIP appear unable to provide detailed information.

When PIP was implemented 10 years ago, it was praised as being on the leading edge of integrated information sharing, and Canada was considered a global leader in the field. While law enforcement can consume information through PIP, there is no means of opening and allowing real time collaboration on a single investigation. In short, law enforcement organizations are seeking a more robust ability to query across RMSs nationally. Study participants lamented repeatedly how far Canada has fallen from its former leadership role in this regard, stressing that PIP was now, technologically, a generation behind where it needed to be. Stakeholders felt that CPIC was similarly antiquated. Anticipated enhancements have not proceeded as planned.

OPTIC Interoperability Challenges

While members of the OPTIC group have full and instant visibility into the occurrences and records across those partner organizations, OPTIC is not without its challenges, the biggest of which seems to be that its governance structure is overly complicated for its users, and thus slow to adapt. To elaborate, if one of the member organizations would like to change something for its jurisdiction, it needs to get agreement from a majority of organizations which is a lengthy, time-consuming process. Secondly, Niche does not connect to other proprietary systems like Intergraph and Versaterm CAD systems, so the link between an organization's Intergraph CAD and the RMS can be unidirectional.

Participants suggested that interfaces be built between key proprietary systems so that other RMS systems could be queried from within the OPTIC cooperative. For example, one of the OPTIC members, Chatham-Kent, is situated an hour away from Windsor and London but cannot query those databases without using PIP, which only returns very limited information. Lastly, the CAD Map is proprietary and dependent on OPP geomatics in Orillia for updates, which update maps on a cost recovery basis, and for OPTIC users that has meant lengthy gaps between upgrades (recently a two-year delay).

Sharing Arrests and Bookings Systems

Arrest and bookings systems are integral to submitting fingerprints, charge info, dispositions to RCMP but there are currently difficulties with automatic interfaces to the RCMP and broader compliance

issues in dealing with the RCMP. Study participants felt strongly that arrest and bookings systems be connected nationally as it would speed the identification process, eliminate time-consuming duplicate data entry, and lead to more consistent data across systems. While some agencies do share mug shots, there is very little consistency even within provinces. Vancouver, for example, has a mugshot database of 150,000 images that law enforcement agents in neighbouring Surrey do not see. This will become an even more galling efficiency gap as law enforcement organizations adopt facial recognition software.

Business Intelligence and RCMP Constraints

RCMP information constraints were noted as key inhibitors to system interoperability, particularly in reference to interconnecting municipal BI databases. Respondents noted that there would be considerable value to being able to run a BI inquiry for a particular city or geography or nationally. Integrating BI systems would result in far better, more accurate, timely situational awareness, but also far less double entry for officers and staff.

RTID

There are a number of challenges to making the RTID more interoperable. A number of custom-built and COTS legacy applications/systems components are integral parts of the RTID system, but in some cases these systems were developed without the benefit of modern technology and standards-based interfaces. These applications and systems are currently being replaced through the RCMP modernization initiatives. Addressing these legacy systems components will provide better interoperability, improved system maintainability, and improved delivery efficiency and reduce support costs.

Interoperability With the Justice System

A troublingly inefficient scenario was noted repeatedly by law enforcement across the country in characterizing the burden of their disclosure obligations. While law enforcement officers typically receive data in digital format (be it a an input from the CAD or RMS, a fingerprint or mugshot, evidence logs from forensics, etc.) the Crown cannot accept the digital material. Officers need to then convert the digital information into a pdf, print it, and physically walk the package to the Crown, which then proceeds to digitally scan and upload the package to its systems. Mugshots are rendered indecipherable; case logs are no longer searchable; speed and evidence quality is lost. Unfortunately this scenario appears to be the rule rather than the exception. Edmonton's police force was able to compel its courts to move to digital by creating a sunset date by which the Crown would no longer receive paper/non-digital formats, in effect forcing the Crown to adapt.

The unnecessary burden the justice system places on policing was a central area of analysis in the recent Report of the Standing Committee on Public Safety and National Security on the Economics of Policing. The archaic and incompatible systems across the justice continuum contribute greatly to cost inefficiencies in policing. This scenario will worsen considerably in the years to come as the traditional workflow stages of an investigation – response, primary investigation, secondary investigation, tertiary investigation, courts and archive – are blend, and the total elapsed time between each stage shortens.

National Information Exchange Model — Compliance and Adoption

By way of background, the National Information Exchange Model (NIEM) is a community-driven, standards-based approach to information exchange which allows a broad spectrum of communities to increase efficiencies and decision making by facilitating the free flow of information across state and city government boundaries.

One of the aims of the study was to assess current state awareness and adoption of NIEM and NIEM-compliant systems. Findings indicate that only 5% of systems are considered NIEM-compliant, meaning that they are poorly predisposed to seamless information sharing. One of the misunderstandings about NIEM is that organizations must unanimously agree on the standards that they will be using; however, by agreeing to a series of information exchange protocol definitions (IEPDs) law enforcement organizations would be able to search across multiple RMS systems. Stated more concretely, if Niche and Versaterm agreed to those exchanges then law enforcement organizations could search for a person search across multiple proprietary RMS systems and geographies.

Lastly, while stakeholders are quick to blame the vendors for lack of action on this front, Niche and Versaterm have said they would support NIEM but customers have not requested it in RFPs; even the latest RCMP RFI only had NIEM compliance as a nice-to-have.

LEGAL AND PRIVACY CONSTRAINTS

As part of the LEIM study, IDC investigated the privacy and legislative landscape to better understand the boundaries, frameworks and barriers (both real and perceived) to information sharing.

While this can be a very nuanced and complicated discussion, there are essentially two central dimensions relevant to the current discussion: the first is understanding the parameters of information sharing among other law enforcement organizations; the second is understanding what, and how, police organizations can or should share information with other ancillary organizations such as social services, health, corrections, and education.

Information Sharing Between Law Enforcement Organizations

With regards to the first area of inquiry, all of the subject matter experts interviewed for this study felt that there was little to no issue with law enforcement organizations sharing information with other police organizations in the course of an investigation. Interviewees cautioned that the law enforcement organization in question needed to have the authority to request a given piece of information, and were against information-sharing where a given law enforcement organization does not have a mandate to request certain information; for example, a corrections employee requesting information from law enforcement systems on another employee as part of an internal human resources dispute. That is to say, our interviewees were clear that information should not be 'repurposed' to ends other than for that which the information was originally intended. This is also directly aligned with the CISC interoperability definition cited earlier in this report.

Legal and Privacy Considerations Among Law Enforcement

The need to share information among law enforcement is recognized in federal, provincial and municipal privacy legislation, and by the various privacy commissioners that enforce it. BC's Privacy Commissioner recently published a comprehensive report on the appropriate use of police records for employment checks. The document contains an analysis of the limits of sharing information by police for employer hiring checks (particularly as it pertains to charges that did not result in convictions and mental health issues), but it also includes strong wording about the central core function of policing and its dependence on thorough and comprehensive information sharing among law enforcement organizations during an investigation.

> "No one disputes that police agencies need broad authority to collect, use, and disclose personal information in order to do their jobs safely and effectively. We depend on them to have accurate, complete and reliable information to investigate crimes, help prosecute criminals and protect the public. In many instances, a police investigation may turn on a seemingly irrelevant piece of information. This is why FIPPA gives police agencies considerable latitude to collect, use, and disclose personal information in performing their duties and functions. Where police agencies use personal information to investigate and help prosecute offences, our criminal justice system contains checks and balances to ensure the accuracy of information." (Investigative Report F14-01 Use of Police Information Checks in British Columbia, Elizabeth Denham, Information and Privacy Commissioner of British Columbia, p. 28)

Multi-Sectoral Information Sharing

The second dimension to information sharing pertains to multi-sectoral or multi-agency information sharing. This has become a matter of interest recently as law enforcement, and community safety stakeholders broadly speaking, have come to recognize that community safety should not be owned solely by the police; multi-agency involvement is not only necessary, but far more effective in terms of keeping at-risk people out of the system.

However, historically, health, social services, education, and so on have operated in isolation from one another, trying to protect the sensitive case information falling under each agency's mandate. Community safety stakeholders feel unequivocally that siloed information systems cause harm by keeping isolated agencies uninformed and only partially cognizant of the total story; early intervention is both ineffective and nearly impossible. Police in particular feel overwhelmed by the resources they have at their disposal, and the number of calls for service that would likely be handled better by experts in adjacent areas of expertise. When people conceptualize community safety they typically think of it as the domain of police work but it is comprised of, and needs to be addressed by, a much broader group of stakeholders beyond police and corrections, including healthcare, education, social services, housing, and the municipality in question. Many of the cases that today fall into the wheelhouse of law enforcement likely shouldn't, or at least should be handled in partnership.

The HUB Project

The province of Saskatchewan has spearheaded a new approach to information sharing and multi-agency community safety. Having had the worst crime rate in Canada eight years running, the Government of Saskatchewan commissioned a study in 2008 on the future of policing. While it was originally thought that the study would lead to an overhaul of the policing system, the study's conclusion was that the Province needed to take a different, holistic, multi-sectoral approach to addressing the issue of its marginalized populations. In so doing the Province established a whole of government approach to risk reduction and early intervention, called 'building partnerships to reduce crime' which tied together nine ministries of government (social services, education, health, housing, justice, police, etc.) with the eight largest police services under the Saskatchewan charter and integrated them into a multi-sector, collaborative risk-driven approach to crime reduction and community care.

The central focus was to look at the key drivers of the core of police work, in order to stop the trend towards increased calls for service in the face of dwindling public safety budgets, and, as importantly, to be able to consolidate the touch points that each involved agency would have regarding a given household or individual, so that interventions could happen earlier and at-risk individuals could be kept out of the system long-term. The ultimate goal of the project was to collect enough intelligence on key 'predictors' to provide agencies with early intervention indicators. The intent is summed up nicely by the Deputy Minister of Corrections and Policing, Dale McFee: "If we can predict, we can prevent." The Province of Saskatchewan refers to its multi-sectoral information sharing arrangements as 'HUB' tables; the approach was later ported over to Ontario, though under the name 'situation tables.' The May 2014 Report on the Economics of Policing reiterates the need to take a broader approach to community safety: "Through its witnesses, the Committee has identified the following primary drivers of policing costs today, namely: an increase in call volume due to social disorder and mental health issues, the changing nature of crime, increasing police sector compensation and the demands placed by the criminal justice system on the police."

Prior to HUB-type implementations, there had been complex case protocols where agencies would intervene collectively once it was determined a given organization could not handle it singularly, but the problem with that methodology was that the chain of managerial support and sign-off was so lengthy that by the time agreement was reached it was well beyond the point where there could be a timely impact.

While not directly correlated, the year following the HUB table implementation in Prince Albert Saskatchewan, the city's calls for service declined by roughly 10% or 666 calls, and its crime stats declined by 11%. The 308 cases brought to the HUB table in one year in Prince Albert assigned to the following domains: 40 were housing-related; 33 maintenance-related; 16 domestic; 31 mental health-related; 47 addictions related; 106 child welfare cases; and 35 were tagged as miscellaneous.

Multi-Agency Privacy and Legislative Reviews

Both Saskatchewan and Ontario have established multi-agency systems and in so doing have conducted far-reaching reviews of their province's privacy legislation to determine how best to proceed while working with the original intent and spirit of the privacy laws. Stakeholders in Saskatchewan's HUB project reviewed all applicable legislation from all three jurisdictions, including FIPPA, PIPEDA,

HIPAA, the Child Services Act, etc. Subject matter experts in both provinces stated that while there are certainly privacy provisions which instruct where one is unable to share information, there are also explicit instructions about when there is in fact an obligation to share as it is in the interest of the betterment of the individual. For example, the Child Services legislation is very explicit about the obligation to share information when there is a risk to a child. Similar statutes exist in other agency agreements as well. This has led to a province-wide shift in Saskatchewan with senior political leadership now committed to implementing an enterprise approach to case resolution, and stating the following: "We've reviewed the legislation. The legislation says you're more than capable of sharing information for the betterment of the clients and we encourage the act of sharing of information for the betterment of the client within the regulations." HUB projects act within the spirit and the legality of the privacy legislation as it was written.

RECOMMENDATIONS

Create a National Strategy

- Canadian police agencies need a national law enforcement information management strategy and roadmap.
- Law enforcement needs to stop thinking parochially, and more as provincial/regional/national enterprises.
- Leverage procurement economies of scale: consolidate datacentre management; share social media analytics licenses; share digital evidence management solutions.
- Research the possibility of creating a national public safety cloud.

PIP 2.0/PRP

- While PIP and CPIC provide some of the information officers need for investigations, and while there are regional pockets of integrated systems such as the OPTIC group in Ontario and BC's PRIME system, there is a need to further integrate key common data systems such as CAD, RMS, MCM and bookings systems nationally.
- PIP 2.0/PRP should have a master name reconciliation capacity, leveraging analytics to eliminate multiple entries of the same person. Alerts need to be used when the same name or address is being searched multiple times.
- PIP 2.0/PRP needs to be able to query on all RMS systems at the granular level ('tattoo on right shoulder').
- PIP should be connected with provincial driver's license databases, drawing on driver's license pictures, and consolidated with national mugshots database.

Standards/Interfaces

- CACP and its partners should strongly encourage use of standards and NIEM-based systems to promote interoperability of existing system investments.
- Key interfaces and information exchange protocols need to be developed between large systems.
- Leverage procurement power to encourage large CAD and RMS vendors to create interfaces and/or information exchange protocols.

- Law enforcement organizations need to embed standards-based solutions into their requirements in procurements.
- Fund the creation of a series of IEPDs between major proprietary systems.
- The CACP should work collectively to compel the vendor community to base their solutions on accepted standards such as NIEM.

Mugshots

- Mugshots need to be centralized and published to the PIP 2.0/PRP. If arrest/booking/mugshot and evidence systems feed into the RMS then only the RMS would need to be interoperable. Doing so would benefit court disclosure, reduce data entry, aid data consistency, negate jurisdictional barriers and lead to more timely investigation and response.

MCM

- Explore feasibility of connecting MCM solutions between provinces (PowerCase in Ontario, PRIME) and to national MCM systems (E&R3 and PIP 2.0/PRP).

RMS

- PRIME BC should connect to ICBC so that ICBC would get all of its data for traffic incidents in real time and would reduce manual reporting by the agencies. Law enforcement would benefit from an interface from Versaterm to ViClas to prevent double entry.
- RMS systems need to be connected to all municipal, provincial, and federal intelligence systems, PIP 2.0, provincial justice systems, provincial transportation systems to access photos, and other regional and national RMS systems. This would result in increased situational awareness, better patrol deployment, integration with provincial justice systems, predictive policing, the consolidation of disparate information sources, and create cost savings by eliminating duplicate data entry.
- Local RMS systems should be connected to the RTID and LiveScan systems.
- Master Name Index and incident collation.

CAD

- CAD systems should be connected to other emergency services (fire and EMS), provincial transportation photo databases, data warehouses and the provincial courts.

BI

- BI systems need to be connected at minimum to regional RMS systems to reduce data entry, and provide better, more complete information and enhanced situational awareness.
- Connect E&R3 (in its current and future states) with larger BI, Big Data and social media implementations nationally.

Digital Evidence Management/Business Intelligence

- Law enforcement BI tools and data should be leveraged internally with other departments in the same municipality; municipal data sources could be fed into the law enforcement BI.
- Digital evidence management systems should be shared regionally/nationally, functioning as one-stop-information-shopping marts.
- Dispositions from court should come back digitally into the RMS.

APPENDIX A

List of Participating Organizations

Vancouver Police Department	Halifax Regional Police
Durham Regional Police Service	Peel Regional Police
Toronto Police Service	Waterloo Regional Police Service
Windsor Police Service	Ontario Provincial Police
Edmonton Police Service	Medicine Hat Police Service
Abbotsford Police Department	Victoria Police Department
RCMP	Saint John Police Force
Niagara Regional Police Service	York Regional Police Service
Service de Police de la Ville de Montréal	Saskatoon Police Service
Regina Police Service	Surrey RCMP Detachment
Central Saanich Police Service	Winnipeg Police Service
Fredericton Police Service	Royal Newfoundland Constabulary
Kentville Police Service	Chatham-Kent Police Service
Halton Regional Police Service	Hamilton Police Service
Kingston Police Service	London Police Service
North Bay Police Service	Ottawa Police Service
Thunder Bay Police Service	Summerside Police Service
Combined Forces Special Enforcement Unit	Service de police de Gatineau
Service de police de la Ville de Québec	Calgary Police Service
Charlottetown Police Service	

Source: IDC, 2014

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world''s leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com