

### **ARCHIVED - Archiving Content**

### **Archived Content**

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

### ARCHIVÉE - Contenu archivé

### Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request. Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.





# Police Information Sharing in Canada Balancing Security, Efficiency and Collaboration

by Marcel-Eugène LeBeuf, Ph.D., RCMP and Simon Paré, M. Ed., RCMP, Ottawa, October 2003

Research and Evaluation Branch Report Community, Contract and Aboriginal Policing Services Directorate Royal Canadian Mounted Police Ottawa 2005

The views expressed are those of the authors and are not necessarily those of the Royal Canadian Mounted Police or the Canadian Association of Chiefs of Police.

Catalogue No.: PS64-8/2005E-PDF ISBN 0-662-40019-4



Royal Canadian Gendarmerie royale Mounted Police du Canada



### Table of Contents

Highlightsiii
Introduction5
How is Information Shared6
Technology versus Trust14
Why Share Information?19
What is Shared?21
Conclusion23
Reference
Appendix 125
Table 1: Description of survey sample6
Table 2: Method of communication
Table 3: Sharing/Using databases/RMS8
Table 4: Is the method of communication influenced by the information shared         9
Table 5: How often police officers share their information with colleagues:         11
Table 6: Regional information sharing with colleagues who are analysts or civilians         12
Table 7: Trust and IT security14
Table 8: Importance of knowing the recipient15
Table 9: IT Equipment16
Table 10: Legal rules and policies17
Table 11: Why police officers share19
Table 12: What they share21

Successful policing depends on information sharing – both within a police force and without. Police routinely exchange information and communicate with colleagues, other police services, members of the public and with political representatives. Recent experiences such as the September 11 terrorist attack have underlined the importance of information sharing, but they have also reminded us about the importance of information security. How are police services responding to these conflicting pressures? This report details the results of a 2003 survey to assess information sharing and its relationship to information technology. Results were compared with a similar 2000 survey.

The survey was designed to complement the November 2003 Conference on Information Sharing held in Montreal under the auspices of the Canadian Association of Chiefs of Police.

## Highlights

All police services depend upon multidirectional information sharing. Everyone, from managers to police officers to support staff, relies on the dissemination of accurate and timely information to do his or her job. This survey shows that there is a relationship between how this information is shared and the nature of the information itself. When security is at issue, face-to-face communications are increasingly preferred.

#### How is information shared?

Although it is increasingly supported by technology, policing is still a relationship-based occupation. This affects information sharing, particularly when the information is deemed sensitive.

Face-to-face contact is the preferred way of sharing information within organizations; telephone is the second choice. Outside the organization, when face-to-face contact is less convenient, telephone ranks first and less direct tools such as email, fax and regular mail are the second choice.

Only about a third of police respondents answer information requests by granting access to departmental databanks. However more than half of police officers use records management systems (RMS). Just over a third have access to others' RMS. Linking databases and allowing queries to other forces' RMS would facilitate ease of access to information and therefore information sharing.

Which tools are chosen to share information is driven to some extent by the nature of the information itself. If police deem the information sensitive or requiring a paper trail, information sharing is more formal and less personal. Furthermore, some information is only available in printed form.

#### How often is information shared?

As expected, police communicate most frequently with fellow workers in their own organization. Frequency falls from very frequent (98 or 99% scoring *always* or *often*) within the organization to less frequent (72 to 90% scoring *seldom* or *often*) for those who are outside their immediate circle (anyone outside the organization, the public and colleagues who are civilians, analysts or other professions).

Municipal police are most likely to share information outside the unit or organization. This may be because their units or organizations are smaller and because they are more frequently in direct contact with outsiders.

#### **Technology versus trust**

Police culture is based on relationships with partners and law enforcement colleagues. However personal knowledge is not always possible when exchanging information. Information sharing faces a real challenge if police officers and law enforcement agencies need to know each other before they start sharing information.

Can technology help assure police that information can be shared securely? Overall, police officers show a high percentage of trust in IT communication systems (87%). System security and even email security were not seen as obstacles to the sharing of information. For example, even though half the municipal police officers expressed distrust in email, 88% used it.

A more important factor is whether information providers know the recipient – 69% said they only share information if they trust the recipient. This is understandable given that police officers learn at the academy, and are encouraged in the field, to build a trusting relationship with colleagues and partners to ensure security.

#### **Response to requests**

The volume of information available to the police at any one time is staggering. Therefore the ability to discern what is being requested and to filter available information for a quick response is imperative. The survey confirmed that respondents selected information for sharing primarily on their judgement of how useful information would be, rather than what had been requested or what was available.

However, almost all respondents said that they did not hoard information. Their routine included collecting information, managing it and releasing it to increase efficiency. Release of information is not restricted to a requestbased or "need to know" system of sharing.

Despite this commitment to efficiency, there is still a tendency to pass on information that is perceived to be useful, rather than routinely forwarding all intelligence to a central source or databank.

#### Conclusion

We can conclude that trusting technology is a higher predictor for sharing information than is trust of the recipient. Therefore, it is essential that organizations develop and promote secure systems as a step to shifting information sharing from a system based on personal initiative to one based on systematic methods.

Rules and regulations guide, rather than obstruct, information sharing. A large percentage of respondents shared information because they have the permission to share. They are also concerned with efficiency and the value of information to the recipient.

Records management systems entail routine reporting and filing of information in a database, increasing information exchange and accessibility. However, human will and/or judgement are determining how, where and to whom information is shared.

Given these factors and the culture of trusting relationships on which policing is built, it is essential to set clear standards and procedures for sharing. Ultimately, a secure and systematic protocol for sharing information – one that is not dependent upon personal initiative or judgement – is essential to build a robust and useful shared database.

## Introduction

Successful policing depends on information sharing – both within a police force and without. Police exchange information and communicate with colleagues, other police services, members of the public and with political representatives. Recent experiences such as the September 11 terrorist attack have underlined the importance of information sharing, but they have also reminded us about the importance of information security. How are police services responding to these conflicting pressures? This report details the results of a 2003 RCMP survey to assess information sharing and how access to information technology facilitates sharing. Our objective was to ascertain how the law enforcement community shared information with colleagues within their own organization, as well as with interested parties from the outside. It was planned to compare these results with those of a similar survey conducted in 2000 (LeBeuf, Paré, Belzile, 2000).

The survey was used as the foundation paper for the November 2003 Conference on Information Sharing held in Montreal under the auspices of the Canadian Association of Chiefs of Police (CACP).

#### Methodology

The questionnaire was sent in May 2003. Depending on available technology, the questionnaire was distributed by regular mail, by fax and electronically by the CACP; it was also available on the CACP web site. Respondents had the option of returning completed surveys by email, regular mail or fax. Recipients included municipal police departments across Canada, many RCMP detachments and such law enforcement partners such as the Department of National Defence, Organized Crime Agency of British Columbia, CN Police and ViaRail. Both managers and front-line workers were encouraged to respond. A follow-up was sent in June 2003,

We received 242 responses from police departments (Table 1). The 1 non-police response and 2 responses from the Royal Newfoundland Constabulary were grouped with the 128 responses from municipal departments for the purposes of analysis. There were 111 responses from the RCMP (including contract police services in seven provinces and the federal police). These are listed as "federal" in the data. Most responses (63%) are from managers, 37% were from front-line workers.

#### Table 1: Description of survey sample

	Municipal	Federal	Total
Number	131	111	242
Percentage (%)	54	46	100

#### **Sharing of Information**

Information sharing is complex and relates to many human and technological issues. Sometimes these factors are linked, in other cases they are not. The variety of ways and means of sharing information reflects available technology. (See Appendix 1 for a list of current initiatives across Canada,) To depict the current state of sharing of information within and outside police departments, we evaluated how police officers share their information within and outside their organization. What influences sharing of information and what are the obstacles and/or incentives to the preferred methods? We were also interested in why they share information and what they did share.

Our goal was to show the intricacies of information sharing and the incentives and disincentives for doing so. We were interested in knowing whether information sharing is integrated into daily routine – much the same as patrolling city streets– or whether it is shared on a need-to-know basis.

## How is Information Shared

Police managers and front-line workers share information continuously through their work day. Communication ranges from recording evidence to personal conversations. Each act of communication can be defined according to these variables:

- n who or what is the target
- n how information is communicated (including whether technology is used)
- n whether communication is spontaneous/systematic and informal/formal
- n whether the communication responds to a request or is volunteered
- n what is the content (including issues of complexity, security and sensitivity)

A briefing, for example, may be systematic in that it is part of standard procedure but delivered informally (verbally and face-to-face) or formally (printed briefing notes).

The RCMP was interested in asking police officers and managers to define such variables. We were interested in knowing how they exchanged information (in terms of frequency, preferred methods etc.) and whether the content or method chosen influenced the degree to which information was exchanged.

Because it is so important to effectiveness and planned response, we were interested in knowing whether information sharing was becoming a systematic part of police work or whether it depended upon the initiative of individuals.

#### How is information shared inside and outside organizations?

Overall, face-to-face communication remains the most frequent (96%) method of sharing information inside an organization. (Table 2) The penetration of information technology at the federal level is demonstrated by a 100% response for sharing information by email, but federal police are strong users of all options (face-to-face, email, fax and regular mail) inside and outside the organization. This is understandable, given the size of the RCMP.

Municipal respondents reserve fax and regular mail for outside contacts. Within the organization, their second choices are email and telephone.

What may be surprising is the low rate at which information is shared via databanks. Though most organizations maintain an information database at some level, giving access to the databank is an infrequent choice – about a third of the time for inside contacts and down to a quarter of the time for outside contacts.

	Overall (%)		Munici	pal (%)	Federal (%)	
	Inside	Outside	Inside	Outside	Inside	Outside
In person	96	83	96	82	96	86
Email	95	85	90	88	100	81
Telephone	83	96	75	99	93	94
Fax	58	91	32	92	88	90
Regular mail	57	86	29	90	91	93
Access to in-house databank	35	23	32	22	38	24

#### Table 2: Method of communication

#### What they said:

(Numbers in parentheses indicate that more than one respondent made the same comment.)

- n Absolutely necessary to verify the recipient first (2)
- n Necessary to make sure only the appropriate person receives the information (2)
- n We have lists of recipients already set up (2)
- n It depends if the person is a member or a civilian
- n Database is password-protected to restrict access
- n I prefer conveying in person when it is sensitive (7)
- n Sensitive information is sent via secure mail (4)
- n We don't use the fax for sensitive information
- n Volume dictates method
- n I have access to enough databanks as it is now (2)
- n Right now I don't have access to all the databanks from my organization

*Record management systems* (RMS) are a systematic way to collect and give access to information via a central databank. More than half of respondents (59%) use RMS, but only a third of those can query other organizations' RMS. (Table 3) Fewer federal respondents share information via RMS.

#### Table 3: Sharing/Using databases/RMS

	Overall (%)	Municipal (%)	Federal (%)
Share by giving access to their databanks	35	32	38
Would share more if they had access to more databanks	34	46	21
Use their organization's RMS	59	66	49
Can query other organizations' RMS	36	37	34

#### Comment:

Overall, direct interpersonal contact (in person and telephone) is the first choice for information sharing within and outside organizations. Email technology has wide acceptance and is used to facilitate information both inside and outside organizations. Fax and regular mail are the second choice for communication outside organizations. Few respondents shared information via databanks.

Municipal police officers see a greater need to share databank information and wanted access to more databanks. This suggests that municipal services would benefit from the linking of current databanks to facilitate information access. Increased database access was not seen as a priority for federal respondents.

The data show that officers do benefit when their organizations implement RMS, which facilitate access and integration of data. Although RMS are complex, costly and may take years to implement, they allow organizations to circumvent integration of current databanks. RMS can contribute to information sharing on the organizational, regional and provincial levels.

#### **Information-Sharing Methods**

We wanted to see if the method of communication chosen depends on the content of the information shared. Responses reflected stringent federal protocols for dealing with sensitive or security-related content. Over 90% of federal respondents agreed that content determined how they chose to share information inside or outside the organization. This compares with 76% for municipal services for sharing within and 81% for sharing outside the organization. (Table 4)

	Overall (%)		Munici	pal (%)	Federal (%)	
	Yes	No	Yes	No	Yes	No
Within the organization	83	17	76	24	92	8
Outside the organization	88	12	81	19	95	5

Table 4: Is the method of communication influenced by the information shared

- n Depends on sensitivity of information (23)
- n Sensitive information only in person (7), only via secure mail (4), with secure fax (2); also cannot be conveyed by telephone; never email; with secure channels; not with faxes
- n Depends on urgency of information to be shared (14)
- n Distinction between formal process requiring paper trail (hard copy) and informal communication (3); also some information is available in hard copy only (3)
- n Depends on the number of recipients (2)
- n Depends on ability of recipient to receive

#### Comment:

The fact that there is a difference between methods chosen for inside and outside suggests that information sharing is not systematic and depends on personal initiative. Other issues include the sensitivity of information, urgency and whether a paper trail is required.

#### **Frequency of information sharing**

Frequency of information sharing with colleagues at different levels of proximity and expertise was evaluated, as was the effect of geographic location.

	Overall (%)			Municipal (%)			Federal (%)					
	Never	Seldom	Often	Always	Never	Seldom	Often	Always	Never	Seldom	Often	Always
From their unit	0	1	31	68	1	1	35	64	0	1	27	72
From their organization	0	2	47	51	0	2	44	54	0	2	50	48
From outside their organization	1	29	58	13	1	30	60	9	1	26	56	16
Who have different expertise	1	34	53	13	1	34	56	9	1	33	49	17
Who are analysts	10	35	37	18	14	38	34	13	6	32	40	23
Who are civilians	10	39	36	15	13	40	35	12	6	37	39	18

#### Table 5: How often police officers share their information with colleagues

#### How often police officers share their information with colleagues:

- n **From their unit:** Trust among unit officers is very high; information is shared with them always or often. (Table 5)
- From their organization: Once again, information sharing at the organizational level is high;
   it is slightly lower for federal police, who are dealing with a much larger organization. (Table 5)
- n From outside: Police share information frequently (about 70% often or always) with colleagues outside their organization; about 30% of respondents seldom or never share information with those outside. (Table 5)
- **With different expertise:** About a third of the time police officers choose not to share their information with non police officers. (Table 5)
- N With analysts: The data suggest that analysts and police officers are not communicating as often as they might. Federal police are more accustomed to working with analysts than are municipal police.

N With civilians: Information sharing with civilians is not systematic (as shown by the low number who always shared with them). Civilians, like analysts, are not the first choice for information sharing. Police give them information often or seldom, but rarely always. About 10% never share information with civilians. (Table 5)

#### How does geographic location affect information sharing?

When information sharing with analyst and civilian colleagues is examined more closely, it becomes clear that there is no systematic national program for information sharing. Over 50% of police in the Atlantic Provinces, Ontario and Prairie Provinces always or often share information with analysts. Police officers from Quebec (20%) and British Columbia (14%) are notable for never sharing information with analysts.

When it comes to sharing information with civilians, there is a gradual erosion in rates of sharing for Atlantic Provinces, Quebec and Prairie Provinces, however there is a stronger tendency to share information with civilians than with analysts in Ontario, British Columbia and, in particular, Yukon, Nunavut and NW Territories. The three areas shared always or often at rates of 70%, 59% and 86% respectively. This compares with Quebec never sharing (24%) and seldom sharing (56%) for a negative total of 80%. (Table 6)

	Analysts (%)				Civilians (%)			
	Never	Seldom	Often	Always	Never	Seldom	Often	Always
Atlantic Provinces	3	39	45	13	13	33	44	10
Ontario	10	34	26	30	0	30	41	29
Quebec	20	34	37	10	24	56	15	5
Prairie Provinces	7	30	43	20	14	43	29	14
British Columbia	14	38	40	8	3	38	54	5
Yukon, Nunavut and NW Territories	0	57	29	14	0	14	57	29
Overall	10	35	37	18	10	39	36	15

#### Table 6: Regional information sharing with colleagues who are analysts or civilians

#### Comment:

As expected, police share most frequently with their own units and within their organizations. Frequency (and, we can assume, confidence or perceived need) erodes with each degree of separation from the unit. The fact that frequency is a little higher for sharing with outside organizations than with those of different expertise suggests that the "outsiders" are other police officers. It is apparent that analysts and civilians are not first choices for sharing information; this is a little more so at the municipal level.

#### **Conclusion:**

Trust and efficiency seem to be the important determinants of whether police will share information. Police choose their tools for information sharing based on content, security issues and whether the recipient is inside or outside his/her organization.

The preferred method of sharing information is personally – either face-to-face or by telephone.

The data suggest that police officers who choose to use email or fax to share information with outside organizations are communicating with people they already know.

Information sharing happens as a result of personal initiative; it is not systematic.

Less personal, nonelective methods of sharing information such as granting access to a database are chosen only a third of the time (32 % for municipal and 38% federal).

## Technology versus Trust

Given the preference for personal modes of communication, is security a factor in information sharing? If so, what are the perceived obstacles to using less personal methods?

#### Does the security of communication systems influence the sharing of information?

The security of information technology systems (computers and networks) is not a major concern for police officers, 87% of whom rated IT as trusted always or often. However, this confidence does not extend to email; only 61% of respondents trusted electronic mail often or always. More federal police officers (69%) trusted email than did municipal workers (54%). The difference is confidence may be related to the prevalence of encryption tools. Almost all (94%) of federal police and only 57% of municipal police had access to encryption technology. (Table 7)

Despite municipal scepticism about email security, it should be noted that this was still one of their preferred means of sharing information with (more or less 90% in Table 2). It seems that the convenience of email wins out over questions about its security or the lack of encryption technology. Conversely, federal officers who trust email more and who have access to encryption technology, use it less frequently.

	Overall (%)	Municipal (%)	Federal (%)
Trust IT security	87	87	87
Trust email security	61	54	69
Use email to share outside	85	88	81
Have access to encryption tools	75	57	94

#### Table 7: Trust and IT security

- n There is no 100% secure system -- we need to manage risk (7)
- n We have a secure infrastructure, but it is difficult to share with other organizations who do not have a secure infrastructure
- n Sharing would be a lot easier if we had the same universal encryption software
- n We need a secure fax

#### **Comment:**

This survey suggests that IT security alone is not itself sufficient to prevent sharing of information – efficiency is a more important issue.

#### Knowing the recipient – is familiarity a factor in information sharing?

Familiarity with the recipient of information is certainly a factor in whether information is shared. However, it is a stronger determinant for municipal than for federal police officers. Again, the size of the organization may require federal workers to communicate more frequently with strangers. About two-thirds needed to know the recipient before sharing information within their organization. This is matched by their prerequisite to trust the recipient before sharing information (67%).

However, the data change when recipients are asked about sharing information outside the organization. Federal respondents were less confident doing so (71%) and municipal police more so (59%), however federal police did not necessarily share more information even if they did know the recipient (61% positive versus 78% positive for municipal police). (Table 8)

	Overall (%)	Municipal (%)	Federal (%)
Say they have to know the recipient before sending information internally	62	63	60
Say they have to know the recipient before sending information outside the organization	65	59	71
Say they share more information when they know the recipient	70	78	61
Say they share only if they trust the recipient	67	67	67

#### Table 8: Importance of knowing the recipient

- n It is absolutely necessary to verify the recipient first (2)
- n It is necessary to make sure only the appropriate person receives the information (2)
- n With trust I know what the recipient will do with the information (2)
- n It feels better when I know the recipient
- n I have to know the recipient or somebody who knows the him/her
- n There are no assured security standards in place, so personal knowledge of the recipient's position and integrity is critical to the decision to allow the process

- n It depends on if the person is a member or a civilian
- n A lot of information is sent to a unit, not an individual

#### **Comment:**

The important finding here is that 65% of police officers overall (59% and 71% respectively) need to know the recipient before sharing information outside their organization. (Table 8) This attitude should be interpreted in light of the training that police receive. From the start, police officers are told that a secure work environment is built on trusting relationships with colleagues and partners.

Though understandable, this could be an obstacle to developing comprehensive shared databases regionally, provincially, nationally and globally.

Is trusting the recipient more important than trusting the technology? Respondents rated both as important but a much higher percentage of police officers rated technology secure (with the exception of email). We can conclude that trusting technology is a higher predictor for sharing information than is trust of the recipient. Therefore, it is essential that organizations develop and promote secure systems as a step to shifting information sharing from a system based on personal initiative to one based on systematic methods.

#### Better access to secure technology and equipment?

When asked if better access to secure technology would increase information sharing, only a third of municipal respondents and a quarter of federal respondents agreed that it would. Federal services already have access to multiple secure tools to share information within and outside their organization. (Table 9)

#### Table 9: IT Equipment

	Overall (%)	Municipal (%)	Federal (%)
Say they would share more if they had more secure/better IT equipment	31	34	26

- n What we have now is good (6)
- n IT has nothing to do with the amount of information shared (5)
- n It would only be quicker (5)
- n If we were certain the information was available only to other police agencies, we would share more information

- n Current infrastructure limits the quantity of data that can be shared
- n We need a secure fax

#### Are legal rules and regulations perceived as obstacles?

Police information sharing is governed not just by personal initiatives but by internal procedures or rules and by legislation such as the *Privacy Act*. Unwritten policies related to police culture may also govern information-sharing behaviour.

Virtually all police officers stated that they take the *Privacy Act* and other legislation, such as the *Municipal Freedom of Information Act*, into consideration when sharing information. The same applies to rules and regulations from police organizations. (Table 10)

#### Table 10: Legal rules and policies

	Overall (%)	Municipal (%)	Federal (%)
Take the <i>Privacy Act</i> and other legislation, such as the <i>Municipal Freedom of</i> <i>Information Act</i> , into consideration when sharing information	95	94	97

Respondent justifications:

- n Third party rule (7)
- n I always ask my boss (9)
- n Access to information (2)
- n I cannot send sensitive or protected information to non law enforcement agencies (2)
- n The Freedom of Information Act and policies govern what we do (2)
- n Our policies prohibit many communications via the Internet
- n Not relevant when we share with other police departments

Sixty per cent of municipal and 69% of federal police said they share only when they have permission. However, as the following comments show, information sharing hinges not on getting permission but on working efficiently and giving mutual aid.

#### What they said:

- n At times, the need to share information supersedes the rules (2)
- n I check with the owner/author of the information (2)
- n I use my judgement (2)
- n Nothing leaves my desk unless the recipient is entitled to it-no wink-wink
- n Certain projects require confidentiality
- It has happened that I did not have permission, but the information was given to someone I trusted greatly and who I knew would greatly benefit from it in his investigation

#### Comment:

The sharing of information remains in the hands of individuals rather than belonging to a formal organizational process. The comment of two respondents, "I use my judgement" implies that building trust, communicating personally and evaluating the needs of those requesting information is a common framework for deciding whether to share information.

#### Conclusion

It is clear that information sharing depends not just on regulations but on judgement and issues of trust. There is little automatic sharing of information. Overall, police officers trust IT communication systems (87% overall) (Table 7). However, both municipal and federal officers are more likely to share information when they know and trust the recipient. This applies equally to managers and front-line officers.

Giving police access to more and better technology was not seen as a prerequisite to increased information sharing. Trust remains the prime factor.

Due to their culture of security and their respect for regulations, police tend to be self-censoring. Rules and regulations must explicitly demonstrate when, how and if police can share information. Otherwise, they will not do so.

## Why Share Information?

Is information sharing based on individual judgement or is it a systematic function within the organization? How is information sharing influenced by the confines and secrecy of intelligence units? There are many reasons why a police officer should engage in information sharing. Some of them were translated into questions:

	Overall (%)	Municipal (%)	Federal (%)
They share only when they receive a request	10	13	6
Sometimes they share only to maintain a good relationship	23	16	31
They share to be more efficient	95	94	96
They share only because the recipient has given them information before or will in the future	4	2	6

#### Table 11: Why police officers share

#### I share only when I receive a request.

Almost all respondents (90%) denied this (Table 11). Most felt that if there were no restrictions, information should be made available.

- n If I am not sharing, I am not doing my job
- n We share information with other agencies on a continual basis
- n I try to be proactive in determining who might find the information beneficial
- n I will never neglect my duty by not giving information when I should
- n How is the other agency supposed to know that I have this information
- n We automatically send reports to organizations
- n The holder of information often fails to recognize the value of it to others. Where it is *releasable*, it should be made available to anyone who has a right to see it

#### Comment:

Data suggests that police are oriented to collecting information, managing it and, according to needs and priorities, releasing it. This does not support the view that police only release information when prompted.

#### I share to maintain a good relationship

Three-quarters of respondents (77%) deny that they use information to maintain working relationships but information has long been a foundation for building trust. This is less evident at the municipal level, where relationships may be less complex, than at the federal level where a third (31%) of the respondents agreed that information sharing is used to maintain relationships (Table 11).

#### I share to be more efficient

Efficiency evoked a strong response in the respondent, 95% of whom agreed that information sharing helped achieve results. (Table 11)

#### What they said:

- n Sharing allows others to make informed decisions (2)
- n Sometimes other agencies will make better use of information
- n As a supervisor, I have to pass the information along to the appropriate person
- n We are intelligence-led, therefore information must be immediately shared with our partners
- n There is always someone who will be able to use your information to save time and effort; sharing is a win-win strategy

#### I share only because the recipient has given me information before or will in the future.

Most respondents (96%) rejected the notion that information was currency to be traded for influence or access. (Table 11) Sharing was not seen as dependent upon getting a return on the "investment" but it was hinted that others may operate this way.

- n That would be counter-productive
- n Right now we share with everyone, even those who do not share anything with us
- n Sharing is not dependent on an equal exchange of items basis
- n Stop being childish–I do not care if a cop never gives me information. Unfortunately, that is what too many cops work by and use as gossip. As a result, too much good information never flows in, and some investigations never progress due to that.

- n We would be happier if we could have increased two-way sharing of information with agencies such as the RCMP. As it is, information sharing is not always reciprocal.
- n Sharing is not a quid pro quo situation; doing so would be an organizational liability and increase risk of failure. Aside from also being the right thing to do, reciprocating drives the motivation for information sharing in my view.

#### Conclusion

Efficiency is the strongest motivator for police sharing information. If this is true, how does it factor into their preference for sharing information with known individuals? (Table 8) It is possible that two cultures are at play – the traditional police culture based on interdependent relationships and the modern police culture that values efficiency above personal obligations. Whichever it is, based on questions 1 and 4 (see tables 1 and 4), we can say that if police officers want to know the recipient to share information (70%), it does not mean the exchange is based on obligation, on a give-and-take relationship, or even a sustained relationship.

The data show that the value of information is not linked to individual/personal attributes. It confirms that information sharing is an ongoing process that is never complete.

### What is Shared?

It has been established that information sharing entails judgement as well as following standard procedures or strictly in response to requests. What influence does content have on police information sharing? Once again, efficiency is thematic; in most cases (58%) police officers provide what is believed to be useful, compared to "what is requested" (26%) and "everything on hand" (16%) Any information filtering is more likely due to sympathy for the recipient than any desire to withhold information. (Table 12)

	Overall (%)	Municipal (%)	Federal (%)
Nothing	0	1	0
What is requested	26	24	29
What they believe to be useful	58	60	55
Everything they have	16	15	16

#### Table 12: What they share

#### What they said:

n Sometimes I do not share information because it is unnecessary to others and they already have enough on their plate.

#### Comment:

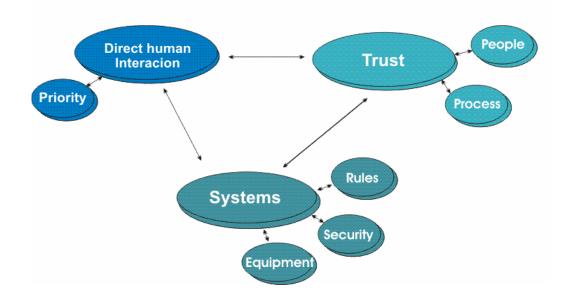
The data suggests that requests are translated in terms of efficiency. All available information for a request is not provided. Therefore, we can infer that it seems that requests for information should be as precise and detailed as possible.

## Conclusion

This survey suggests that at least three interconnected factors have a direct impact on the sharing of information among Canadian police officers:

- 1. Personal human contact is the preferred mode of information sharing
- 2. Knowledge of and trust in the recipient and information technology increases rates of information transfer
- 3. Support in the form of clear guidance for when, how and if information can be shared and give police permission to do so. (See below.)

Given these factors and the culture of trusting relationships on which policing is built, it is essential to develop and promote secure technologies for information transfer, and to set clear standards and procedures for sharing. Ultimately, a secure and systematic protocol for sharing information – one that is not dependent upon personal initiative or judgement – is essential to build a robust and useful shared database.



## **Current Factors Affecting Sharing of Information**

## Reference

LeBeuf, M.E., Paré, S.; Belzile, M. (2000). Canadian Police Information Technologies: Current Overview. Ottawa: Canadian Police College. Available at: www.cpc.gc.ca

# Appendix 1

### Information Sharing Initiatives across Canada

#### **Atlantic Provinces**

- n An initiative is underway in New Brunswick to link databanks through an automated system that will allow for access to police databanks within the province.
- n PIMITS Police Information Management/Information Technology Sharing project links police computer systems, including municipal, RCMP and regional departments. The mandate of this project is to seek and develop methods of sharing information among the various police agencies in the province.
- n Restructuring of CISNB
- n We have an integrated information-sharing unit.
- n The development of PROS by the RCMP throughout the province, the installation of Versaterm by Halifax along with the development of an Internet database developed by the province for the retention of Emergency Protection Orders issued under the *Domestic Violence Intervention Act.*
- n We currently have a memorandum of understanding with RCMP "B" Division to share information. We provide access to our Integrated Constabulary Automated Network and they provide us with access to PIRS.
- n The RNC is involved in the Justice Knowledge Network initiative and is working with policelearn.com.
- CIS Nova Scotia provides a vehicle to share information throughout the province with all law enforcement agencies.

#### Ontario

- Our analysts get together with CISO and produce a provincial threat assessment, which is presented to the chiefs every year.
- The London Police Department has spearheaded an initiative to share information provincially with a view to federal sharing. This project is starting with small successes and building on them. London, Windsor and Ottawa will be the first, with Toronto following shortly thereafter.
- OPTIC We automatically share our information with 42 municipal departments and the OPP.

- Working closely with CSIS in exchanging information and putting a new system in place to electronically share information.
- Intelligence publishes a bi-weekly newsletter with crime information and officer safety bulletins that go on the Intranet for access by other members.
- A new computer system makes front-line sharing easy for our region (Waterloo, Brantford, Stratford, Guelph) and gives access to each other's Intranet and message boards.
- We have a memorandum of understanding with DOJ, CIC, CCRA, DFAIT to search their databases (missing children).
- Partnerships with US Border Patrol, US Coast Guard on cross-border security and smuggling
- CODIS Combined DNA Index System
- The London Police Department has started an initiative to share with Windsor, Ottawa and Toronto.
- Sharing of operational plans and policies and procedures
- Use of email for exchanging information and questions from our city councillors
- We are a member of the CIMS project, which is meant to link our RMS databases together to share information.
- Integrated Justice Project in Ontario. Driven by provincial ministry, includes most municipal police departments and the OPP.

#### Quebec

- JFO on organized crime
- We have developed our own internal RMS and have offered it to other departments who seem interested.
- Tiger Web site to share information on Montreal street gangs
- In Quebec, police departments develop new tools on their own without creating partnerships, therefore everyone does their own little thing.

#### **Prairie Provinces**

 We are presently in the process of obtaining a major case software called RAID – US DOJ.

- CISA has established a routine dissemination protocol wherein information is shared between regular, associate and affiliate members on a daily basis. This is done electronically and via regular mail.
- Rural Crime Watch Talk Mail system allows police to share information with a large part of the community on operational matters as often as they wish.
- Linking our victim services to the Provincial Court database.
- We are setting up a system to share court briefs, photos, digital recordings with the Crown.
- We are setting up a secure communication network with the RCMP Entrust.
- Shared radio channels with other agencies, domestic and international. It appears that we and WPS will soon be on the same platform and I am intrigued by the possibility of an easy technological link between us for our ORS.

#### **British Columbia**

- Video conferencing to send messages from OIC to troops
- The most sharing still happens at Tim Horton's, where we meet late at night with guys from five different departments.
- Police Regional Operational Data Sharing through Law Enforcement Information Portal (LEIP). Integrated Records Management System. Electronic fingerprint capture and classification on-line.

#### Yukon, Nunavut and Northwest Territories

• We are presently looking at ways to share information more effectively with law enforcement agencies in Alaska.

## **Other Reports Available**

Date	<u>Title</u>	Author
2004	Peacekeeping Missions and the Police in Canada: An impact study of civilian police officers and police services	Marcel-Eugène LeBeuf, Ph.D
December 2004	Organized Crime and Human Trafficking in Canada: Tracing Perceptions and Discourses	Christine Bruckert, Ph.D. & Colette Parent, Ph.D.
September 2003	Aboriginal Organized Crime in Canada: Developing a Typology for Understanding and Strategizing Responses	E.J. Dickson-Gilmore, Ph.D. & Chris Whitehead
May 2003	CCTV: Literature Review and Bibliography	Wade Deisman, M.A.
May 2003	Media Coverage of Organized Crime – Police Managers Survey	Judith Dubois
April 2003	Canada and the New Challenges Posed By Corruption in the New World Order: A Literatur Review	Fernando Acosta, Ph.D. e
March 2003	Criminal Networks	Vincent Lemieux, Ph.D.
March 2003	The Direct and Indirect Impacts of Organized Crime on Youth, as Offenders and Victims	Holly Richter-White, M.A.
June 2002	Canada-US Law Enforcement Border Partnership – An Evolving Situation	Marcel-Eugène LeBeuf, Ph.D
June 2002	On Organized crime and police cooperation in the European Union – lessons learned. Interview with Professor Cyrille Fijnaut	Marcel-Eugène LeBeuf, Ph.D
June 2002	Media Coverage of Organized Crime: Impact on Public Opinion	Judith Dubois
June 2002	Trafficking in Human Beings and Organized Crime: A Literature Review	Christine Bruckert, Ph.D. & Colette Parent, Ph.D.
April 2002	Communities, Contraband and Conflict: Considering Restorative Responses to Repairing the Harms Implicit in Smuggling in the Akwesasne Mohawk Nation	E.J. Dickson-Gilmore, Ph.D.
1999	A Report on the Evaluation of RCMP Restorative Justice Initiative: Community Justice Forum as seen by Participants	Jharna Chatterjee, Ph.D.
August 1998	Restorative Justice And Policing In Canada Bringing The Community Into Focus	Margaret Shaw & Frederick Jané