Police Information Systems, Information Practices and Individual Privacy

KATHRYN SCHELLENBERG
Guelph, Ontario

Cet article décrit quelques systèmes communs d'information et des pratiques de la police à la lumière de la législation qui vise à protéger la vie privée des individus. L'auteur montre que le personnel policier est sensible aux droits de la personne et essaie de reduire les menaces posées par l'usage d'informations dont dispose la police. Les menaces sont de plus mitigées par l'absence d'information "soft" dans le système national CIPC et les limites sur la capacité de partage électronique des données des centres locaux. Cependant, l'auteur évoque certaines craintes au sujet de la qualité et de la sécurité des enregistrements, le niveau de qualification, les pratiques en matière d'information et les pressions en vue de relier les centres d'enregistrement locaux. Ces interrogations méritent l'attention des experts en matière de politique.

This article describes some common police information systems and practices in light of legislation designed to protect individual privacy. The author finds that police personnel are sensitive to human rights issues and attempt to reduce threats posed by the use of police information. Threats are further mitigated by a lack of "soft" information in the national Canadian Police Information Centre (CPIC) system and limitations on the ability to share electronically data in local agency records. However, the author also raises concerns about the quality and security of records, the level of training, questionable information practices, and pressures to link local records systems. These concerns merit more focused attention from policy experts.

INTRODUCTION

Canadian policing entered the electronic age in 1972 when the Canadian Police Information Centre (CPIC) went online. CPIC (pronounced see'pick) is an automated system operated by the Royal Canadian Mounted Police (RCMP) on behalf of the nation's policing community. While serving a broad range of police information needs, the RCMP summarizes CPIC's purpose as providing "tactical information on crimes and criminals" (RCMP 1995, no. 17).

In investigating crimes and criminals, the police risk making two types of errors. First, they may believe an innocent person to be guilty of wrongdoing. In the parlance of statistical hypothesis testing, this would be analogous to making a *Type I* error (see Ott, Mendenhall and Larson 1978, pp. 218-20). Conversely, police may falsely believe a guilty person to be innocent of wrongdoing, which would be to commit a *Type II* error.

In principle, systems like CPIC are aimed at reducing both types of errors. However, statistical theory informs us that efforts to reduce one type of error tend to *raise* the risk of committing the other type. Statisticians also stress that it is almost always more serious to commit (more important to avoid) Type I than Type II errors. In the criminal justice

system this premise is reflected in the familiar tenet: "it is better that ten guilty persons go free than that one innocent person be wrongfully punished."

Many civil libertarians worry that the nature and handling of data in police systems raise the risk of Type I errors. Kenneth Laudon (1986), an expert on US systems, cites many examples of individuals who were "wrongfully punished" in that they were falsely arrested and jailed or, more commonly, suffered civil abuses such as being harassed by police, fired from their jobs or denied housing because police data were of poor quality, misinterpreted, or disseminated to persons whose "need to know" was questionable at best (also see Gordon 1986; and Pounder 1986 re information system abuses in the US and UK respectively.)

Canadian privacy expert David Flaherty (1986) observes that negative publicity surrounding abuses of the National Crime Information Center (NCIC) system in the US had a positive spillover effect on CPIC. While arguing for strong oversight of systems and practices, Flaherty notes that CPIC designers tried to avoid the problems that had plagued NCIC. Although the system operated for several years without the "compulsion of law," CPIC set "an impressive example of implementing principles of data protection" (Flaherty 1986, p. 134).

CPIC is now subject to the compulsion of federal law; compatible law governs the information practices of most municipal/provincial police agencies. Statutes are designed to protect individuals from unjust consequences (Type I errors) mainly via privacy safeguards over how agencies collect and use personal information. Recently, however, Canadians have seen initiatives that challenge the validity of privacy protection. Whereas statutes shield criminal history information from public disclosure, victims' rights advocates insist that communities have a "right to know" when persons who pose a threat to public safety are in their midst. Also, a growing number of employers and community organizations are asking job applicants or volunteers to submit to criminal background checks. And in the wake of the Paul Bernardo trial in Ontario, serious questions have been raised about how information is shared or withheld within the policing community itself (A. Campbell 1996).

These developments may give rise to greater scrutiny and debate surrounding systems like CPIC, not only among specialists, but the general public as well. The aim of this article is to help inform the debate for non-specialists by: providing an overview of privacy/information legislation, describing some common police information systems and practices, and highlighting some issues that merit more focused policy consideration.

Information and Privacy Legislation (A Brief Introduction)

The information practices of federal government agencies are governed by the *Privacy Act* and the *Access to Information Act* (Canada 1980*a*; 1980*b*). All the provinces but Prince Edward Island have one or more comparable Acts. Alberta (1996), British Columbia (1992), Nova Scotia (1993), Ontario (1990*a*; 1990*b*), Quebec (1994), and Saskatchewan (1990) have single comprehensive Acts which address both privacy and information issues. Manitoba (1985) and Newfoundland (1981) have separate Acts but issues related to personal privacy are covered by freedom of information statutes. New Brunswick (1995) has an information Act only; issues related to personal privacy are addressed in Acts aimed at specific programs (New Brunswick 1994). The head of each government agency, or an individual designated by the head, is responsible for the practical implementation of the respective Acts. Most Acts provide for external oversight via a privacy and/or information commissioner. While there are important differences among Acts, they share many striking similarities and often use nearly identical wording for certain types of provisions and definitions. Indeed, Canadian law reflects international principles, established in 1981, by the Organization for

Economic Cooperation and Development (see OECD 1994, pp. 68-70; also see Bennett 1991, for cross-national similarities and differences in approaches to electronic privacy law).

In general, Canadian law enshrines the public's right of access to certain kinds of records held by government agencies. At the same time, individual privacy is protected through restrictions on the handling of personal information, including prohibiting disclosure to third parties or the public without the individual's consent. Statutes allow individuals to inspect information about themselves, make corrections and add statements of disagreement over content. If an agency uses information to make decisions that affect an individual, it may be required to retain a record (e.g., for at least one year) so as to give the person an opportunity to obtain access and inspect it (e.g., Alberta 1996, 34[a]).

While most people are unaware of their rights and will never look up data about themselves, it is felt that the existence of information law will lead to better information management (Ontario 1993, ch. 2, p. 5). Also, Acts require agencies to assist individuals in exercising their rights. This includes publishing a guide to information sources. The federal guide is *Info Source;* here the RCMP describes its databanks, what may be disclosed, and how to apply for access (Treasury Board 1995, pp. 763-77). In most jurisdictions, agencies may — in Alberta, British Columbia, and Nova Scotia *must* — assist those who apply for information by "creating" records where none exist if they can do so with "normal computer hardware, and software, and technical expertise and, creating the record would not unreasonably interfere with the operation of the public body" (British Columbia 1992, 6[2][a]).

A head may transfer a request if she or he believes another agency has a greater interest in a record. Normally, an agency has custody or control of records in its possession but confusion can arise if more than one agency has copies of a record (see, e.g., Alberta 1995, pp. 18-19; Ontario 1993, ch. 3, pp. 7-8; Ontario 1994 [FIPPA, s. 10], pp. 5-8). When it comes to "personal" information, it appears that originating agencies retain control. In Ontario, for instance, where one institution has "receipt of personal information disclosed to it by another institution.... The receiving institution may use this personal information only for the purpose for which it was disclosed by the first institution" (1993, ch. 5, p. 9).

Neither access nor privacy rights are absolute and each Act lists several discretionary and mandatory exemptions. Law enforcement agencies may disclose personal information to other agencies, including agencies in foreign countries, where exchange is sanctioned by agreement, treaty or legislative authority. A head may — in some jurisdictions *must* — disclose personal information to the public if there is a compelling public interest that justifies the violation of an individual's privacy. Police agencies might use such provisions to disclose names of persons with a history of child molestation to a register for child-care workers or warn a community about the release of dangerous offenders. The legal validity of all such disclosures has not been fully established (see, e.g., Alberta 1995, pp. 112-14), but recently introduced legislation would give Ontario police chiefs the right to disclose such information without fear of violating provincial information/privacy laws (Girard 1996). On the other hand, agencies may deny access to an applicant's personal information if disclosure would harm or otherwise interfere with law enforcement or investigation. They may even refuse to confirm or deny the mere existence of some records.

The Present Study: Data Collection

This study was part of a two-stage project which examined the impacts of computer-linked technologies on policing. Stage one entailed a qualitative study of *Central Municipal* (pseudonym), a force in the "central" region of the country. Data collection involved reviewing documents, interviewing

approximately 20 individuals from all areas of the force, and spending 20 hours of observation in dispatch/CPIC centres and patrol cars. In addition to the case study, I attended an executive police training seminar on "Policing and the Technological Revolution" as a guest of the Canadian Police College in Ottawa.

Based on the case study and seminar, a 235 item survey covering a broad range of issues was developed and administered in Central Municipal and four other forces — Central Regional, Central Rural, Atlantic Municipal, and Atlantic Regional (pseudonyms). All three central forces are in one province; the Atlantic forces are in two different provinces. The forces reflect considerable diversity in organizational structures, operational policies, technologies, and service demands. Four forces are fairly small, with fewer than 300 (sworn and civilian) members, and serve communities with populations under 200,000. The fifth force is very large but is made up of small detachments that serve rural communities and small towns; four detachments and their shared communications centre participated in the study.

Each force and detachment was visited for one or two days (two to four shifts). The aim of the visits was to have front-line officers, supervisors (sergeants and staff sergeants) and civilians complete the survey, but some members of each force were interviewed as well. Also, I estimate that the opportunity to observe and interact with personnel while they worked contributed between 30 and 40 hours of informal observation and discussion.

The survey was presented on notebook computers (PCS). To protect confidentiality and privacy, respondents were not asked to identify themselves.

Nearly everyone who was invited to take the survey did so, yielding 265 sworn and 88 civilian respondents. The sample of officers appears to be representative of Canadian personnel on characteristics such as age (Campbell *et al*. 1992; Statistics Canada 1992), but senior managers (who were not targeted as survey participants) are underrepresented. Also, since the study was confined to three provinces and excluded large urban centres, I do not claim that these respondents or forces represent Canadian policing in general. However, I have had communications with information/computing specialists in other forces and draw upon their insights to inform the discussion that follows.

Overview of Automated Police Information Systems

Canadian Police Information Centre

CPIC is operated by the RCMP on behalf of some 1,285 separate Canadian police agencies and 1,180 RCMP detachments (RCMP 1995, no. 17). Day-to-day operational policies are set by an advisory committee of senior officers representing agencies from across the country. However, nearly half of the committee members are RCMP, so in practice, that agency establishes CPIC policy (Flaherty 1986).

The CPIC system is a collection of electronic files (databases) which can be accessed via computer terminals linked to the Centre in Ottawa (RCMP 1995, no. 17). Much of the data are supplied by member agencies who have discretion over what information to report, retain responsibility for its accuracy and immediacy, and are "the only one[s] entitled or enabled to alter their records" (Treasury Board 1995, p. 763). Commonly queried RCMP files include:

- Persons: This is the most frequently queried file; it contains data on individuals who are wanted by police, charged, parolees, missing (including children), prohibited from driving or possessing firearms, and others.

- Vehicles: (e.g., stolen or wanted in connection with a crime).

- Property: (e.g., guns, stolen articles).

- Criminal History Records (CHRs) maintained by the RCMP Criminal History Section.

Besides RCMP databases, CPIC provides access to provincial motor vehicle and drivers' licence data, the US NCIC system, and state driver/vehicle databases. Foreign agencies have reciprocal access to CPIC, but criminal history information is reviewed by an RCMP Interpol employee before it is released to a foreign agency (Privacy Commissioner 1996). Finally, CPIC lets agencies post "alerts" and exchange narrative messages.

In addition to CPIC, the RCMP operates specialized systems. One is the Automated Criminal Intelligence Information System (ACIIS) maintained by the Criminal Intelligence Service Canada (CISC) network of agencies from across the country. CISC gathers data on organized criminal activities such as "trafficking of illegal drugs, gambling, extortion ... and contract murder" (RCMP 1995, no. 26; Treasury Board 1995, pp. 764, 773). Another system, the Violent Crime Linkage Analysis System (ViCLAS) offers trained specialists a sophisticated analytical tool to identify similarities in crimes committed across the country (Backgrounder to Campbell 1996). Access to ACIIS and ViCLAS is highly restricted and in some areas the systems are not heavily utilized. Ontario forces, for instance, gained access to ViCLAS a few years ago but, until recently, only a fraction of murders and serious sexual assaults were reported to the system. CPIC on the other hand, is relatively visible and widely used.

When CPIC was introduced, the police community greeted it with enthusiasm. Within two hours of going online, the Ontario Provincial Police (OPP) submitted the plate number of a burned out (stolen) vehicle and recorded the system's first "hit" (Higley 1984, p. 492). That year, Central Municipal's annual report declared that, "with the speed of transportation by air, the criminal was getting ahead of us, but we are now closing the gap with [CPIC]." In the first full year of operation, Central Municipal submitted an average of 5,000 queries a month or about 54 per officer. More recently, CPIC was queried more than 35 million times in a three-month period. Based on a population of 76,368 officers (Statistics Canada 1995) this translates to 160 queries per officer per month. Some officers in this study claimed to consult the system between 15 and 20 times on average during a typical (10 to 12 hour) shift.

From a human rights perspective, criminal history records are the most sensitive of the commonly queried files. Except for cases involving young offenders, police agencies and courts are not obligated to report all criminal cases to the RCMP but most agencies do send reports and the Criminal History Section has approximately two and a half million records (Privacy Commissioner 1996). Put another way, about one in ten Canadians is represented in the CHR database. The RCMP purges about 117,000 of its CHR files each year; purging criteria depend on the type of offense and Act under which it was prosecuted (see Privacy Commissioner, pp. 14-17; 20).

Yearly, the CHR database is queried about 22 million times via CPIC (Privacy Commissioner 1996, p. 20). If a CHR record exists, the full record contains "tombstone" data (e.g., name, date of birth), physical characteristics, aliases, a "list of all [reported] charges and dispositions" including: acquittals, dismissals, (unpardoned) convictions and cautionary warnings (p. 5). "Cautions" are supplied by initiating agencies to alert other agencies if an individual might be violent, suicidal, etc. Most queries do not seek the full record; about 80 percent ask for the Criminal Name Index (CNI) which simply names (and cautions) unpardoned persons who have been charged under the Criminal Code and fingerprinted, or the Criminal Record Synopsis (CRS) which reports tombstone information and criminal convictions only.

In the early years of CPIC operation, access was restricted with passwords and, in some forces, by prohibiting physical space around terminals.

Officers in the field submitted coded requests via radio to operators at the station. Where they had direct access, many officers were too intimidated to use the system. By the early 1980s, queries still had to be typed into a hardcopy terminal and the system was very sensitive to protocol errors. One officer described early technical training as "scare tactics over making mistakes; people were terrified of putting a colon in the wrong place."

Today, the system is much friendlier and many terminals in every police station provide easy access. Some searches still require considerable expertise but most officers perform at least some, if not most, of their own queries. It is especially easy to submit queries in forces where cruisers have mobile data terminals (MDTs) which provide remote access to CPIC. (Of the forces in this study, Atlantic Municipal and Central Municipal have MDTs.) In at least one force, the detailed contents of criminal histories cannot be accessed via MDT, but routinely queried databases are available. Two years after Central Municipal got MDTs, queries were up by about 50 percent over pre-MDT years (similar findings are reported by McRae and McDavid 1988; Layne 1990; Palys, Boyanowsky and Dutton 1984). Some civil libertarians have expressed concern over the growing ease of access to sensitive data but Flaherty (1986) observed that the privacy of MDT compared to radio communications about identifiable individuals offers an important benefit in protecting civil liberties.

A number of CPIC features enhance civil liberties (Flaherty 1986). The range of authorized users is narrower than for the US NCIC system and data are less likely to fall into the hands of unauthorized individuals who are more prone to misinterpret or misuse the information (e.g., landlords and employers). Further, the system is more of a guide to information than a source. While a force may put arrest warrant data on the system, the warrant itself stays with the originating agency. Also, records in the system tend to be brief and contain little of what Flaherty calls "soft" information.

But CPIC is not devoid of soft information. For example, a number of officers interviewed here expressed concern that once a *caution* (e.g., violent) is put into a criminal history record, it always stays there. This is worrisome since a person can be labeled based on the judgement of one officer. Also, dispositions that are overturned by appeal may not be reflected in a CHR. This is because local agencies provide the input for CHRs but tend not to be involved in appeals; thus they may not know of and report the new disposition to the RCMP (Privacy Commissioner 1996, p. 6).

Despite these concerns, CPIC is respected by police personnel and outsiders. Flaherty (1986) expressed more concern over local systems, claiming they had received insufficient external scrutiny and standards may be weak as a result.

Local (Agency) Records Systems

While there are no truly paperless records systems, Central Rural and Central Regional had largely replaced paper records with electronic files by the time this study was conducted. Central Municipal, Atlantic Municipal, and Atlantic Regional had only skeletal summaries in electronic format (Central Municipal has since moved toward full automation).

Some large forces have exclusive use of their records systems but all of these forces participate in sharing arrangements. Central Municipal and Atlantic Municipal each cooperate with a small number of forces in neighbouring jurisdictions; Atlantic Regional uses a system run by the RCMP; Central Rural and Central Regional belong to a technology cooperative of more than 60 agencies. These two forces are separated by hundreds of kilometres, yet they can access each other's highly detailed records.

Unless forces share a system, the ability to exchange electronic data is limited; this problem is exacerbated by some forces' unwillingness to share information. Some years ago, senior police officials in Ontario urged the government to strengthen

interagency information links by developing a compatible province-wide system (Campbell *et al*. 1992).

This proposal raises some human rights concerns as local records contain sensitive, often impressionistic, open-ended information on a wide range of individuals who come into contact with the police. Ericson (1982) argues that police data are "molded and pruned" so as to convey certain impressions about individuals. Personnel in this study saw the likelihood of deliberate distortion as small, but shared Ericson's view that data do not simply reflect objective facts. As one detective observed, computer files lead to mental images which can unfairly bias attitudes toward victims and witnesses as well as suspects.

Due to the harm that could arise from sensitive data, forces may limit external access to some files. To protect victim privacy, for instance, one force in this study restricts other agencies' access to detailed contents of sexual assault files. A privacy/freedom of information specialist in another force with a shared system stated that if an individual applies for access to personal data submitted by more than one force, the force will not release information contributed by other forces. Moreover, the force would not release personal information to a third party, even if the individual consented to its release.

Integrity of Systems and Information

Survey respondents saw police computing in a very favourable light and felt electronic data generally create fair, accurate impressions about people. A strong majority believed that police access to data benefits the public by improving decision making. Over 70 percent of officers felt that unrestricted police access to detailed criminal records would reduce the likelihood of false arrests (Type I errors). On the other hand, 94 percent of all respondents thought it would be a bad idea to give landlords, employers, etc. access to the kind of information in police databases. However, interview and survey results also pointed to areas of potential concern.

Due to the recognized high quality in RCMP information practices (Thacker *et al*. 1987), that agency has established technical, procedural, administrative, and security standards for information technology used by federal agencies (1992*a;* 1992*b*). In their manual for "small" systems, they identify the common problem of personnel who "do not have an information processing background and thus are often not aware of ... vulnerabilities ... [with the result that data] may be inadequately protected" (1992*b*, pp. 1-2).

Although some officers have considerable computing ability, few have the professional "information processing background" implied here, especially in small forces. Even large forces (systems) have encountered vulnerability problems. A knowledgeable insider claimed that security was woefully weak when the large system used by Central Regional and Central Rural first went into operation. In part, this was because the civilian designers did not see the need to subject police users to standard security measures like audit trails. Flaherty (1986) describes less than adequate auditing when CPIC was relatively new, enabling an operator to engage in illegal use of the system. More recently, an officer in British Columbia was alleged to have used CPIC to identify owners of cars parked near abortion clinics and then passed their names and addresses to anti-abortion activists. The federal Privacy Commissioner's office (1996, p.12) concluded that CPIC access to criminal history records was open to misuse, but also stated that some (unspecified) problems encountered in the past should be eliminated by a new version of CPIC under development.

Although security problems seem to be addressed as they arise, other concerns stem from legitimate uses of police systems. CPIC and local systems do not offer powerful analytical capabilities. The interpretation and analysis of information depend

greatly on the skill and judgement of the user. Officers receive formal and on-the-job CPIC training, but according to civilians and officers who were interviewed, there is a need for better training and support. In the words of one civilian specialist, "before you can become an officer, you have to know self-defense, how to shoot, and life-saving, but *nothing* about computerized data handling, computer systems, or record systems."

The assessment seems overstated, but on a survey question that asked respondents to rate their knowledge/expertise on CPIC (1 = none; 5 = high), only 16 percent of officers, compared to 31 percent of civilians, gave themselves a 5. Most officers gave themselves 4 (36 percent) or 3 (34 percent). For local systems, 40 percent of officers (and civilians) with highly automated records (Central Rural and Central Regional) gave themselves a 5, but only 20 percent of officers in less automated forces were so confident. Reference materials could also be improved. Less than 5 percent of all respondents rated written computer documentation as excellent; 22 percent said it was good; nearly 40 percent said it was poor. Interviewees claimed that the multivolume CPIC manual contains instructional errors and that much of its content is "unintelligible."

Moving from expertise to data quality, the various Canadian information and privacy Acts require agencies to make every reasonable effort to ensure that personal information is accurate, complete and up-to-date, especially if it will be used to make decisions that affect the individual.[1] These concerns are reflected in CPIC policy and the RCMP has rigorous procedures to ensure the accuracy of information it makes available through CPIC. Indeed, so far as criminal history data are concerned, the office of the federal Privacy Commissioner concluded that employees in the Criminal History Section were keenly aware of the potential impacts of errors in criminal records and that:

> Although no system can provide 100 percent assurance that errors will not occur ... the RCMP has ... more than adequate processes and procedures to ensure that most errors are discovered and corrected before the information is released to users. The author also could not think of any additional procedures that would assist the RCMP in reducing the possibility of errors (1996, p. 8).

Local agencies are accountable for the integrity of the information they put on CPIC. The RCMP demands regular audits to ensure that records are backed by documentation to establish their accuracy and validity. Users are warned not to assume the validity of records; "hits" must not be used as substitutes for judgement, and must be verified against original records. Still, the sheer volume of data means that the RCMP has to rely on contributing agencies as to its integrity (Privacy Commissioner 1996). CPIC specialists interviewed here claimed that forces vary widely in the quality of data they put on the system and in their approaches to information handling. Such claims raise questions about local systems.

Several study participants complained about local systems that are archaic, inflexible, and difficult to use. Some highly skilled officers in one force said their system was overly demanding and unable to accept data that did not conform to flawed built-in assumptions (e.g., that all forces process arrests in the same way or that all incidents occur on land with a unique street address). Users sometimes devise inventive methods to get the computer to accept data but they also worry that this might unintentionally distort its *meaning*.

Samples of respondents were asked to rate CPIC, local, and provincial driver/vehicle records on five indicators of data quality[2]: *completeness*, *accuracy*, *level of detail*, *vulnerability* (to unlawful access), and whether codes/terms *make sense*. For the making sense criterion, respondents were also asked to rate NCIC records and the driver/vehicle records of "other" provinces. (The criterion of whether old information is appropriately purged was inadvertently omitted.) (Mainly civilian) records specialists and

CPIC operators were given at least four criteria; other respondents were each given one of the five criteria.

Responses suggest records are fairly accurate, complete, intelligible, and secure but there is room for considerable improvement. Table 1 reports the percentage of respondents who gave "good" ratings on each of the criteria presented. CPIC received the highest ratings with 75 percent, 63 percent and 53 percent of respondents giving good ratings for accuracy, completeness, and low vulnerability respectively. Ratings for local records were markedly lower. In general, there were no major differences in how forces rated their own records on completeness or detail but the *least automated* force gave its records the lowest scores for accuracy.

Except for CPIC records, civilians gave lower ratings than officers for completeness. Only 30 percent of civilians gave "other" forces on shared systems high ratings on completeness; they also gave other forces lower marks for accuracy. Fewer than half of the officers gave any local system a good mark for security. (On a related question, 45 percent of all respondents felt computer records are more vulnerable to unlawful access than paper records.)

Respondents claim the information in CPIC, local records, and same province driver/vehicle records makes sense to them. On CPIC records there is a substantial difference between civilians (80 percent) and officers (65 percent). Since civilians tend to have more CPIC expertise, their higher rating is

TABLE 1

Percentage of Respondents Who Gave Good Marks[1] to Five Aspects of Data Quality in Selected Automated Police Records Systems (Percentages are based on samples of sworn and civilian employees)

Type of System and Records	*Completeness (n=129)*	*Accuracy (n=120)*	*Detail (n=124)*	*Vulnerability (n=118)*	*Make Sense (n=84)*
CPIC records	63.0	75.4	64.2	53.4[2]	71.2[2]
Records of respondents' own force	48.0[3]	61.8	58.4	47.5[2]	71.6[4]
Records of other forces on shared local system	41.9[3]	51.3	61.8	45.6	61.1
Driver/vehicle records of respondents' province[5]	51.1[3]	52.1	63.7	41.9	65.1
Driver/vehicle records of other provinces	—	—	—	—	27.4
NCIC (US) records	—	—	—	—	26.9

NOTES:

1. Response categories ranged from 1 (low) to 5 (high). A "good mark" = 4 or 5 (out of 5) for completion, accuracy, and making sense; 1 or 2 for (low) vulnerability, and 3 for detail (neither too little nor too much).
2. There is a 10%+ difference between officer and civilian ratings with more civilians giving good marks.
3. There is a 15%+ difference between officer and civilian ratings with more officers giving good marks.
4. There is a 10%+ difference between officer and civilian ratings with more officers giving good marks.
5. One force is omitted here because provincial driver/vehicle records were not fully computerized at the time the survey was conducted.

understandable, but considering that officers make decisions based on these data, we might wish for greater comprehension. There is broad agreement that NCIC records and out-of-province driver/vehicle records are relatively *unintelligible*.

Information Attitudes and Practices[3]

Whether data can serve legitimate police needs and protect civil liberties depends in part on how it is used. In a criminal investigation or other situation where there are clear grounds to suspect an individual of wrongdoing, officers gather as much information as possible. In arrest situations, searches are especially thorough so as to reduce the risk of a wrong decision. A suspect's criminal history may be taken into account in deciding whether or what type of charge is laid; interviewees felt, however, that if information were very old or related to "minor things" it would not be unfairly prejudicial (i.e., raise the risk of a Type I error).

The majority of database queries do not involve arrest situations; often, they do not even reflect a suspicion of criminal wrongdoing. In many forces, officers are expected to submit some type of query on most, if not all, persons they deal with in an official capacity. For example, citizens who are stopped for a routine traffic violation might expect the officer to query their vehicle and driver's licence. These are not controversial searches from a civil liberties perspective. But from an officer's perspective, traffic stops pose more risk than is appreciated by the public since speeding or erratic driving may signal involvement in a criminal activity. Therefore, officers often check the CPIC Persons file. Some query the criminal name index (CNI) as well, but others balk at going this far. As one constable explained, he "needs to know" if a car is stolen, if a driver has a valid licence, and if there is a warrant for his/her arrest, but not whether he or she has ever been charged with an offense in the past. Thus, he felt that querying the CNI would be an unjustified invasion of the driver's privacy.

To explore officers' feelings about privacy, survey respondents were asked to imagine pulling over a vehicle for a routine traffic violation and finding out the driver was a personal acquaintance. They were told they had no reason to suspect the driver of any other offense and asked if they would submit queries (1 = definitely yes; 5 = definitely not). Fewer than 5 percent chose 1 for any type of query. Most chose 5 or 4 (definitely/probably not). Specifically, the percentages who said "no" (i.e., chose a 5 or 4 response) were: driver's licence (65 percent); vehicle (70 percent); Persons file (74 percent) and CNI (80 percent). Officers with MDTs were less opposed to querying the driver's licence or vehicle but more than half resisted. Resistance to checking the Persons and CNI files was especially strong among Atlantic Regional officers.

Concern for privacy aside, officers might forego submitting queries for other reasons. Flaherty (1986) cites the case of a man charged with obstruction after scuffling with police over being detained to run a CPIC check. A judge overturned the charge, arguing that it is illegal to detain an individual to run a query "unless there is an arrest or police procedure or investigation under way" (p. 137).

Technical limitations also affect the number of queries officers submit. On the survey, nearly half indicated they would "definitely" query more and 30 percent would "probably" query more if response time were faster. Even with MDTs, officers (77 percent) curtail CPIC requests due to slow turnaround time; in many forces, MDTs cannot access local records at all. Officers who submit requests through operators at the station see time-delay problems as acute. In one force, response time was increasing, queries were on the decline as a result, and people "who don't look like they need running, probably won't be run."

This observation raises questions about how officers decide which people "look like" they need running. Marx (1988) has criticized "predictive" practices such as using "profiles" to decide who to

pull over on the highway or search. Predictive policing has a long history. In the 1960s, Central Municipal reported that for years officers had randomly checked cars and drivers, especially "strangers ... at odd times ... and in odd locations." The *Charter of Rights and Freedoms* prohibits such searches today (Griffiths and Verdun-Jones 1994, pp. 116-26; Yates and Yates 1993, pp. 131-32). Officers can search CPIC, however, and in doing so, may find "grounds" to conduct a physical search.

The same profiles arouse suspicion now as in the past. Interviewees claimed that female or "clean-cut" drivers in newer, "family-type" cars are less likely to get checked; young males and drivers in out-of-town cars at 3:00 a.m., or older, run-down cars (i.e., the poor and disadvantaged) are more likely to be checked.

A controversial variant of predictive policing is "cold querying" vehicles such as cars parked at motels frequented by drug dealers or out-of-town cars at shopping malls. This can lead to useful information, such as identifying a vehicle wanted in connection with a crime; usually, it simply identifies a car's owner who can then be queried on other databases. Some forces frown on the practice due to questions about its utility and/or concerns about privacy rights. However, a widely held view that police officers can never have too much information, hardly predisposes them to curb data collection activities (a concern raised by Flaherty 1986). In one force, some supervisors encouraged cold querying by using the monitoring capabilities of the automated dispatch/MDT system to track the number of queries submitted by individual officers as a measure of their productivity.

Emerging Trends and Issues

Although the findings reported here are only exploratory, they suggest that police personnel are sensitive to and try to reduce human rights threats posed by information in automated systems. Threats are further mitigated by a lack of detail and soft information in records which can be widely accessed as well as technical limits on the ability to electronically share information in local records. Still, the findings also suggest that the level of data quality and security in some systems, along with some questionable practices, present a risk of Type I errors. The risk is presumed to be small, but nonetheless real. Moreover, a number of emerging trends threaten to raise the risks that individuals may suffer unjust consequences arising from police information. Two trends — increasing pressure to share information among police agencies and growing demands to release information to third parties and the public — are discussed briefly here.

In recent months, questions about police information practices have been framed by scathing criticism over horrific *Type II* errors — especially the case of serial rapist-murderer Paul Bernardo in Ontario. Mr. Justice Archie Campbell's (1996) review of this case cites several information-related problems which facilitated Bernardo's ability to elude police. For example, Toronto police had thousands of leads about the serial "Scarborough" rapist, but the paper-driven process could not link tips about individual suspects (viz., Bernardo). After Bernardo moved and raped a woman in St. Catharine's, police put a zone alert on CPIC, but that system could not link the case to the cases in Scarborough. The Green Ribbon Task Force (GRTF) which investigated the murders of Leslie Mahaffy and Kristen French did not have a case management system to classify the flood of leads. Police also failed to pay serious attention to women who reported being stalked. One victim gave police a wrong licence plate number, but when another victim gave the right number, a computer search identified Bernardo. The search did not turn up other incriminating data on him and the officer did not pursue the lead or file a report on the complaint. Two days after Kristen French was kidnapped, the correct plate number was again reported to police who did not act on it because they were looking for a Camaro at the time (Bernardo drove a Nissan).

Palys *et al*. (1984) found that police tend to overrely on computer data at the expense of other sources, including what the person in question might say. When officers acted on a tip and spoke to Bernardo in the French investigation, they did not regard him as a serious suspect, partly because of his "cooperation and the wedding pictures on the wall" (Cairns *et al*. 1996, p. 19). All the missed leads led Campbell to wonder "how many times Bernardo had to be reported ... before ... all the information was put together" (1996, p. 33).

Campbell also examined the actions of non-police actors such as the coroner who did not recognize foul play in the death of Bernardo's sister-in-law. Ontario government directives now stress a need for coroners and pathologists to "think dirty" in death investigations (Backgrounder to Campbell 1996, p. 11).

Finally, the case was plagued by rivalries. Even after Toronto Police had convincing (DNA) evidence that Bernardo was the Scarborough rapist, they did not pass this information to the GRTF. A lack of interagency coordination and cooperation was so severe that Justice Campbell said that they may as well have been operating in different countries.

To prevent future errors, Campbell proposed sweeping reforms in police information practices when investigating serious serial crimes. Ontario's Solicitor General praised the proposals, stressing that the province had already taken steps to ensure "the highest level of police cooperation and information sharing" (p. 2 of News Release re Campbell 1996). Just months after Bernardo was charged, the OPP set up a ViCLAS system linked to the RCMP system. Campbell urged *mandatory* reporting of murders and serious sexual assaults to ViCLAS; the province agreed. It also agreed to have forces adopt common computerized case management technology which will allow them to compare information, and it will set up a multiagency body of specialists to investigate serious serial crimes. Finally, the province will soon test an Electronic Information Sharing Project which will let forces run their records systems on any computer platform. The pilot project will link several large agencies; queries will result in summary reports of all incidents involving an individual or vehicle in all participating agencies. This may be the first step toward achieving Campbell's eventual goal of standardizing other "information and records systems" (1996, p. 64).

Hopefully, such measures will reduce Type II errors involving predatory, mobile criminals. But in theory, the risk of Type I errors will rise with intensified efforts to reduce Type II errors. This raises concerns about how reforms might affect the routine information practices of rank and file officers. While one can only speculate at this point, changes in some official and informal attitudes and behaviours seem probable.

Officers handle numerous situations which, in their judgement, do not merit an official report. With hindsight from the Bernardo case, more situations will be documented. A case in point is that all claims of stalking would now seem to require a formal report (Campbell 1996, pp. 27-29, 54). Also, factors that predispose police to be suspicious may be more inclusive in the future: that is, like pathologists and coroners, officers may feel pressured to "think dirty" toward persons and situations that would not have aroused their suspicion in the past. More persons will "look like they need querying" and be searched on more databases than before. These practices will be facilitated as more forces move toward full records automation and acquire MDTs and other remote access technologies.

In many areas, it is now possible to "cold query" a car and learn (via CPIC) whether the car's owner has a valid driver's licence, has ever faced criminal charges in the past, is currently wanted by police, and (from local records) whether she or he has been a criminal suspect, victim, or witness, or tends to file noisy party complaints. As local systems become linked, information could feasibly be available for anywhere a person has lived in Canada.

Along with the growing volume and accessibility of data, the police face mounting pressures to release information to volunteer organizations, employers, and communities. These pressures are illustrated by two recent developments covered in the press.

The first is the proposed Ontario bill that will give police greater freedom to warn communities when dangerous offenders are released on parole or bail (Girard 1996). The legislation is in response to a recommendation arising from an inquest into the death of Christopher Stephenson, an 11-year old boy who was murdered by a repeat sex offender. Girard reports that the bill was praised by Jim Stephenson, Christopher's father, and by Priscilla de Villiers whose daughter Nina was murdered by a dangerous offender and who founded CAVEAT, a victims' rights organization. The second illustrative development is the Western Hockey League's (WHL) announcement that it plans to ask "all personnel who have any contact with players" to sign a release form authorizing the RCMP to run criminal background checks (MacLeod 1997, p. A1). The plan is in response to the recent conviction of coach Graham James for sexually assaulting two players over a period of years (MacLeod 1997). Other minor hockey leagues may follow the WHL's lead.

Canadian employers cannot obtain access to criminal history data directly, but one of the reasons why 3,700 or so individuals apply for copies of their criminal history records each year is to meet employment screening requirements (Privacy Commissioner 1996, pp. 9, 20). Although local agencies have access to CHR files through CPIC, the tendency is to refer applicants to the RCMP (Ontario 1993; Privacy Commissioner 1996). If they insist on getting the record from the OPP or Ottawa-Carlton Regional Police (and presumably, other forces as well) they will receive a copy of only: "those charges that the police force in question has processed. The police force will never provide information about charges that have been processed by another police force" (Privacy Commissioner 1996; p. 9).

Those who request a copy of their CHR from the RCMP receive the full record; they can also ask for a report that relates only to convictions or, if there are no convictions, can obtain a letter to this effect. In some cases, individuals may authorize the RCMP to release information to third parties. In these cases, the institution usually provides tombstone information which the RCMP uses to search the CNI. If the finding is positive, the institution is advised that a CHR "may" exist; to obtain further information, it must then submit the individual's signed fingerprints (Privacy Commissioner 1996).

Obviously, demands to identify individuals with criminal backgrounds reflect a belief that such information will enhance the public safety. However, Graham Stewart, executive director of Ontario's John Howard Society claimed that there is no evidence to support the view that public interest releases will make communities safer (in Girard 1966). We might also ask whether criminal background checks will provide the protection sought by employers and volunteer agencies. Indeed, a search would not have identified Graham James as a threat to young hockey players because he had no prior criminal record (MacLeod 1997). And although organizations may evaluate cases individually (as is the intention of the WHL), background checks could easily lead to unfair treatment of individuals who are found to have a record but do not pose a threat.

Police officers interviewed for this and other studies have expressed concerns about how criminal history information is used. When individuals consent to the release of a record to a third party, RCMP policy is to release the full record. However, "in many instances only information relevant to the employment sought is disclosed ... in order to not adversely affect an individual's employment prospects" (Privacy Commissioner 1996, p. 10). As cited above, one local agency privacy/freedom of information specialist will release information *only* to the individual concerned even if he or she consents to a third-party release. The officer believes that many, if not all, agencies have similar restrictions. The

rationale is that individuals are often not aware of all the data that might exist in a local record or its quality; therefore, records should not be divulged unless the individual is allowed to see (and challenge) their contents.

Some Considerations for Policy Researchers

One concern posed by wider information-sharing is that standards can vary widely from one agency to another. Using criminal history records as an example:

> even if the RCMP purges information from its system and ... advises the contributing agency that the information has been purged, the RCMP has no way of ensuring that the contributing agency has purged the information from their own files and systems ... [and] information concerning an individual's dealings with the criminal justice system could exist in another agency's files long after [it is purged by the RCMP] (Privacy Commissioner 1996; p. 13).

The informational needs of an agency or small group of agencies may justify keeping a record longer, or allowing content with greater detail and subjectivity, than would be acceptable for CPIC precisely because of its national scope. However, linking systems could result in a *de facto* wide-scale system with the kinds of content now curtailed by CPIC policy. This is all the more worrisome as the original meaning of information can become obscured over time and with the geographic, political, and cultural distance from its source.

The prospect of merging systems implies a need for more standard policies and practices. However, as we saw in the case of one system, information standards reflect broader assumptions which may not apply in all forces. A force may experience appreciable disruption if a system's features or policies do not mesh with other operating norms. We should not be surprised, therefore, if the working out of common standards leads to major interagency conflicts.

Decision-making mechanisms pose other problems. If a majority of forces are small, one vote per agency will work against the interests of larger forces. This is reportedly why *none* of Ontario's large municipal or regional forces are members of the system operated by the Ontario Municipal and Provincial Police Information Cooperative (OMPPAC). To give greater voice to large forces could put small agencies at a significant disadvantage.

Questions related to the control and custody of personal information may prove especially contentious. The current premise that originating agencies retain control over records led one review panel to conclude that some information sent to CPIC could not be investigated under the "federal" *Privacy Act* because it was not under the control of the RCMP (Thacker *et al*. 1987, p. 54). But while local agencies retain control in the sense that they decide what to put on, or remove from CPIC, the RCMP has effective control over whether information is disseminated once it is in the system. Thus, when a foreign agency makes a CHR request through CPIC, the information is released or denied by an RCMP employee, not the initiating agency (see Privacy Commissioner 1996, p. 12). Also, an individual who could receive only a partial criminal history record from a local agency will, via a request to the RCMP, obtain access to all portions submitted by any agency.

Since several Acts allow or require agencies to create electronic records for applicants, perhaps "one-stop shopping" should apply to shared data in local systems. This possibility raises the question of whether discretion over disclosures should be extended to any agency with access to the collective information or assigned to a central authority as is the case with criminal history records. The answer may depend on whether information is to be disclosed to the individual to whom it pertains, to

another law enforcement agency, a third party such as an employer, or released in the "public interest."

Critics have attacked statutes that give agencies discretionary power over public interest disclosures — especially if provisions do not "clearly set out the public interests involved and the test[s] to be used" (Information Commissioner 1994, p. 29; also Thacker *et al*. 1987). The criticism reflects a concern that privacy rights may be violated unjustifiably. It was in this spirit that one study concluded that government should act as a "trustee" as opposed to mere "custodian" of personal information (New Brunswick 1994, p. 35). The notion of trusteeship implies the discretion to withhold as well as disclose — and a duty to balance the public's interest in guarding against those who pose a clear and present danger to public safety against its interest in safeguarding the privacy of those who have run afoul of the law but deserve: "a second chance, an opportunity to ... start life anew, regardless of past sins or crimes, to rehabilitate themselves through work and reintegration into the community" (Laudon 1986, p. 114).

In the face of mounting pressure to make more information available to officers, to other police agencies, to employers, and to the public, we might ask how the police can continue to act as trustees in the information-saturated environment on the horizon. This is the basic dilemma policy researchers must address.

Notes

This article is based on a study conducted in 1993 and funded by the *Canadian Police College*. I am thankful to the College for its support and to the five agencies and nearly 400 individuals who were interviewed and/or completed the survey. I am also thankful to Kristine Dawkins, Sharon Duff, Linda Gerber, Hugh Lautard, Donald Loree, Victor Ujimoto and Kenneth Woodside for their advice and assistance at various stages of this project. Address correspondence to: Kathryn Schellenberg, P.O. Box 25093, Guelph, Ontario, N1G 4T4.

[1]Ontario legislation (1990*a*, 40[3]; 1990b, 30[3]) *exempts* personal information collected for law enforcement purposes from the general provision that data not be used unless it is accurate and up-to-date. Although the exemption recognizes that police may have to act based on whatever data are available, it hardly absolves agencies of the duty to maintain high standards of data quality.

[2]Questions and response options regarding *data quality* were as follows:

a. "How would you rate each of the following computer databases with respect to the *completeness* of the information on the system (i.e., how often is information which should be in a record missing)?" For degree of completeness (1 = low; 5 = high).

b. "How would you rate ... databases with respect to the *accuracy* of the information (i.e., is the information correct and up-to-date)?" (1 = low; 5 = high.)

c. "How would you rate ... databases with respect to *level of detail* (i.e., do you get too little or too much information)?" (1 = too little; 5 = too much.)

d. "How would you rate ... databases with respect to the degree of *vulnerability* of the information to unlawful access?" (1 = low; 5 = high.)

e. "How would you rate ... databases with respect to how easy or hard it is to understand the information (i.e., do the codes/terms, etc. used *make sense* to you)?" (1 = no; 5 = yes.)

[3]The information "practices" described here were reported or otherwise identified via interviews and survey responses. While it was not possible to observe most practices directly, the consistency of findings from force to force and with previous research suggest that responses offer a fairly valid reflection of actual behaviour.

References

Alberta (1995), *Freedom of Information and Protection of Privacy: Policy Manual* (Edmonton: Alberta Public Works, Supply and Services).

____ (1996), *Freedom of Information and Protection of Privacy Act*, S.A. c. F-18.5, Office Consolidation.

Bennett, C.J. (1991), "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," *Science, Technology and Human Values* 1:51-69.

British Columbia (1992), *Freedom of Information and Protection of Privacy Act*, S.B.C., c. 61, as amended by S.B.C. 1993, c. 46.

Cairns, A., S. Burnside and C. Blizzard (1996), "The Bernardo Report: No Alarm Bells," *The Toronto Sun*, 11 July, p. 19.

Campbell, A. (1996), [Inline] *Bernardo Investigation Review. Report of Mr. Justice Archie Campbell* (News Release; Backgrounder; Terms of Reference; Summary and Recommendations, 10 July). The Queen's Printer for Ontario. Available on Internet URL: http://www.gov.on.ca/MBS/english/new/index.html.

Campbell, D. S., *et al*. (1992), *A Police Learning System for Ontario: Final Report and Recommendations* (Toronto: Ministry of the Solicitor General, Strategic Planning Committee on Police Training and Education).

Canada (*1980a-81-82-83*), *Access to Information Act*, S.C. c. 111, Sch. 1 "1."

Canada (*1980b-81-82-83*), *Privacy Act*, S.C. c. 111, Sch. 11 "1."

Ericson, R.V. (1982), *Reproducing Order: A Study of Police Patrol Work* (Toronto: University of Toronto Press).

Flaherty, D. (1986), "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police Information Centre," *University of Toronto Law Journal*: 116-48.

Girard, D. (1996), "Sex Offender Alerts on Way," *The Toronto Star*, 11 December, p. A3.

Gordon, D.R. (1986), "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System," *Politics and Society* 15:483-511.

Giffiths, C.J. and S.N. Verdun-Jones (1994), *Canadian Criminal Justice* (Toronto: Harcourt-Brace).

Higley, D.D. (1984), *O.P.P. The History of the Ontario Provincial Police Force* (Toronto: The Queen's Printer).

Information Commissioner of Canada (1994), *The Access to Information Act: A Critical Review* (Ottawa: Minister of Public Works and Government Services of Canada).

Laudon, K. (1986), *Dossier Society: Value Choices in the Design of National Information Systems* (New York: Columbia University Press).

Layne, K. (1990), "Unanticipated Consequences of the Provision of Information: The Experience of the LVMPD," *Journal of Police Science and Administration* 17:20-31.

MacLeod, R. (1997), "WHL to Use RCMP Screening," *The Globe and Mail*, 10 January, pp. A1, A6.

Manitoba (1985-86), *The Freedom of Information Act*, S.M. c. 6 — Cap. F175.

____ (1987), *The Privacy Act*, R.S.M. c. P125.

Marx, G.T. (1988), "The Maximum Security Society" in *New Technologies and Criminal Justice*, ed. M. LeBlanc, P. Tremblay and A. Blumstein (Montreal: Centre Internationale de Criminologie Comparée, Université de Montréal).

McRae, J.J. and J. McDavid (1988), "Computer-based Technology in Police Work: A Benefit-Cost Analysis of a Mobile Digital Communications System," *Journal of Criminal Justice* 16:47-60.

New Brunswick (1978), *Right to Information Act*, S.N.B. c. R-10.3.

____ (1994), *Protecting Privacy in an Information Sharing Environment.* (Fredericton: New Brunswick Task Force on Data Sharing and Protection of Personal Privacy).

____ (1995), *An Act to Amend the Right to Information Act*, S.N.B. c. 51.

Newfoundland (1981*a*), *An Act Respecting Freedom of Information*, c.5.

____ (1981*b*), *An Act Respecting the Protection of Personal Privacy*, c.6.

Nova Scotia (1993), *Freedom of Information and Protection of Privacy Act.* c.5.

Organization for Economic Cooperation and Development (1994), *Privacy and Data Protection: Issues and Challenges* (Paris: OECD).

Ontario (1990*a*), *Freedom of Information and Protection of Privacy Act*, R.S.O. c.F-31, Office Consolidation (April 1995).

____ (1990*b*), *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. c.M-56, Office Consolidation (July 1995).

____ (1993), *Municipal Freedom of Information and Protection of Individual Privacy: Handbook for Municipalities and Local Boards* (Toronto: Management Board of Cabinet, Queen's Printer).

____ (1994), *Ontario Access and Privacy Legislation: Annotations* (Toronto: Management Board of Cabinet, Queen's Printer).

Ott, L., W. Mendenhall and R.F. Larson (1978), *Statistics: A Tool for the Social Sciences* (North Scituate, MA: Duxbury Press).

Palys, T., E.O. Boyanowsky and D.G. Dutton (1984),

"Mobile Data Access Terminals and their Implications for Policing," *Journal of Social Issues* 113-27.

Pounder, C. (1986), "Police Computers and the Metropolitan Police," *Information Age* 8:3-17.

Privacy Commissioner of Canada (1996), *Study of the Criminal History Records as Maintained by the RCMP* (Ottawa: Office of the Privacy Commissioner of Canada).

Quebec (1994), *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information.* R.S.Q. c.A-2.1.

Royal Canadian Mounted Police (1992*a*), *Technical Security Standards for Information Technology* (Ottawa: Supply and Services Canada).

____ (1992*b*), *Small Systems Security Guidelines* (Ottawa: Supply and Services Canada).

____ (1995), *RCMP Fact Sheets 1995* (Ottawa: Public Affairs and Administration Directorate of the RCMP, Supply and Services Canada).

Saskatchewan (1990-91), *Freedom of Information and Protection of Privacy Act.* c.F-22.01.

Statistics Canada (1992), "Police Personnel and Expenditures in Canada," *Juristat Service Bulletin* 12, 20. (Ottawa: Canadian Centre for Justice Statistics).

____ (1995), "Police Personnel and Expenditures in Canada," *Juristat Service Bulletin* 15, 8 (Ottawa: Canadian Centre for Justice Statistics).

Thacker, B.A. *et al*. (1987), *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (Ottawa: The Queen's Printer).

Treasury Board Secretariat (1995), *Info Source: Sources of Federal Government Information 1995-1996* (Ottawa: Supply and Services Canada).

Yates, R.A. and R.W. Yates (1993), *Canada's Legal Environment* (Scarborough: Prentice-Hall).