INVESTIGATION REPORT
INVESTIGATION P95-005

CARS, PEOPLE, AND PRIVACY: ACCESS TO PERSONAL INFORMATION THROUGH THE MOTOR VEHICLE DATA BASE

March 31, 1995

David H. Flaherty
Information and Privacy Commissioner
of British Columbia
4th floor, 1675 Douglas Street
Victoria, British Columbia V8V 1X4
tel. (604) 387-5629
fax. (604) 387-1696

Table of Contents

A. EXECUTIVE SUMMARY

The Office of the Information and Privacy Commissioner anticipates that the publication of this report will lead to greater public awareness about the existence and uses of the Motor Vehicle Database. There are many user groups of the database and while most uses are legally authorized and necessary for the functioning of the motor vehicle registration and insurance system, a very real possibility exists for misuse of the personal information in the system.

The Motor Vehicle Database is maintained by the Ministry of Transportation and Highways. The ministry has legal responsibility for the records of approximately 5.5 million vehicles registered in British Columbia. Approximately 3 million of these vehicles were licensed according to figures for 1994. The range of situations in which the database is consulted may have led many members of the public to assume that it is a public registry in much the same manner as the Land Title Office is currently regarded. This is incorrect. Access to the database, although wide, is circumscribed for specific uses of specific users.

However, wide access, even when allotted for specific use by specific users can still lead to undesirable, even nasty, consequences of personal information abuse, such as women being stalked through information obtained by authorized users conducting unauthorized searches of license plate data. Protection of the personal information (the privacy) of registered vehicle owners, while maintaining efficient access to information for authorized agencies conducting authorized searches, means that there must be a reliable mechanism for detecting and tracing abuses.

This can be accomplished by **audits**. On a regular and repeated basis, there should be both human and electronic scanning of database access. There must be a chain of accountability

where access to personal information is on a "need to know" basis. Further, there should be a means to audit the auditors to ensure that the system and its checks are working as they should.

There should be internally-created **privacy codes** that incorporate appropriate **fair information practices** to provide guidance to user groups on how to handle properly the personal information they access. Such privacy codes would set out standards that identify for all the members of the user group what information can be accessed, how it may be used, why it is important to respect the rights of the information subjects, and how those rights can be respected. At present, privacy codes are used in many areas where legislation does not yet apply, as a means of demonstrating to the public that information users take privacy rights seriously.

Implementation of the recommendations contained in this report will assist in protecting the public. But equally important is that the public be made aware that certain uses of personal information are inappropriate and that the public has a right to object to, and demand the investigation of, any inappropriate use.

B. SUMMARY OF RECOMMENDATIONS

1. The ministry should limit access to the database to those users whose need to obtain access is consistent with the reason for which the database information was gathered in the first instance. The ministry should also examine use of the alpha fiche by the private sector, with emphasis on auditing use of the alpha fiche, and within three months report to this Office its proposed policy for continued or limited access. (Page 7) 2. Where a written agreement does not exist with a user group, such as CPIC, such an agreement should be created, which will lend substance to what may in the past have been appropriate, but unwritten, rules regarding data access and data use. This agreement should incorporate fair information practices as its foundation, consistent with the *Freedom of Information and Protection of Privacy Act*. (Page 9)

3. The Ministry of Transportation and Highways should establish an audit program for compliance with fair information practices with individuals trained and assigned to the specific task of conducting audits of the Motor Vehicle Database user group community. (Page 11)

4. The software employed by ICBC for the Motor Vehicle Database should be re-engineered so that there is a powerful, easily accessible electronic record of all entries into and output from the database, including a record of the number of and type of files consulted. (Page 13)

5. The terms of future agreements with Motor Vehicle Database users and registry companies should be more rigorous, and should specify that non-compliance with the access policy constitutes a fundamental breach of the contract. In addition, all user groups should be required to create and adopt their own privacy codes which will bind all members of the user groups. The privacy codes must have substance, be meaningful, and incorporate the basic principles of privacy protection identified in this report. (Page 13)

6. ICBC, in collaboration with the ministry, should embark on a public education project aimed at informing vehicle registrants of their privacy rights under the *Freedom of Information and Protection of Privacy Act*. The information contained should spell out in clear, understandable language the avenues for launching privacy-related complaints, both within ICBC or the ministry, and to the Office of the Information and Privacy Commissioner. (Page 15)

C. BACKGROUND

1. Introduction

Recent media coverage of the conflict between opposing sides in the abortion debate in Vancouver has focused on a relatively novel development in the controversy: the tracing or accessing of personal information by way of vehicle licence numbers. The possibility of violence in the debate has lent a degree of urgency to the realization that one's personal information, particularly one's name and address, can be obtained through reference to one piece of information which vehicle owners are by law obligated to display: a licence plate number.

2. Scope of the Report

News media attention in this instance has tended to focus on the actions of a certain officer of the Delta Police Department, and possible breach of trust in the use of the Canadian Police Information Centre (CPIC) system to gain access to personal information. The Delta Police Department has referred this specific concern to Crown Counsel for consideration of criminal charges.

This Office has a different focus. We have examined the general issues surrounding personal privacy in a complex, multi-user database. We do not comment on whether the specific actions of the police officer warrant sanctions but address in a more systemic fashion the question of what restrictions, if any, should attach to the use of the Motor Vehicle Database both by other users and by police forces via the CPIC system. The terms of reference for this report are attached as Appendix One.

3. The Motor Vehicle Database

Motor vehicle data are recorded so that the Motor Vehicle Branch of the Ministry of Transportation and Highways ("the ministry") and the Insurance Corporation of British Columbia (ICBC) may properly administer the *Motor Vehicle Act*, the *Insurance (Motor Vehicle) Act*, the *Commercial Transport Act*, and other motor vehicle-related legislation. The name and address of the registered owner of a motor vehicle constitute personal information as defined by the *Freedom of Information and Protection Of Privacy Act* (FOIPPA). Government routinely uses personal information in carrying out its legally mandated functions. The Motor Vehicle Database, which government has constructed, furthers that fundamental purpose.

The ministry has legal responsibility for the records of approximately 5.5 million vehicles registered in British Columbia; approximately 3 million of these vehicles were licensed

according to figures for 1994. In addition to vehicle registration and insurance, the multitude of possible uses for the database include law enforcement, civil litigation, and confirmation of ownership for lending institutions.

Indeed, the Motor Vehicle Database is frequently consulted: approximately 3.3 million search transactions involved access to vehicle information plus personal information, such as the name and address of the registered owner. These transactions originated from police and other law enforcement agencies (2.3 million), from municipalities for collection of parking fines and by-law enforcement (740,000), and private sector enterprises, including registry companies (25,000), towing companies, and parking companies (90,000).

This figure does not include the tens of millions of transactions relating to insurance renewal or claim-related purposes. ICBC's Information and Privacy Manager notes that an inquiries clerk talking to an ICBC customer about a claim could easily complete 10 to 20 data "transactions" in a single interview; each transaction would involve adding to, or obtaining, specific pieces of information from the database.

In addition, ICBC maintains a micro-fiche-based list called the alpha fiche. At present it is distributed to three provincial ministries and eight registry companies. It allows searches using the name of the registered owner; one does not need vehicle information. Thus, armed with an individual's name, individuals with access to the alpha fiche can quickly determine what vehicles are registered to an individual and obtain the corresponding vehicle registration numbers. With the vehicle registration number(s), a user can then search the database for an individual's address. (This particular data transaction would be recorded in ICBC's input and output logs.) While the alpha fiche is not a computer-based system, it is nonetheless quick, powerful, and updated on a weekly basis.

4. The Office of the Information and Privacy Commissioner, the Ministry of Transportation and Highways, and ICBC The ministry and ICBC are both public bodies as defined by the *Freedom of Information and Protection of Privacy Act*. This means that the Office of the Information and Privacy Commissioner (IPC) receives complaints and requests for reviews of decisions by these public bodies to withhold or disclose information. This Office views the current attention to the uses of the database as an opportunity to heighten public awareness of privacy issues associated with access to such a database. We have received the full and energetic co-operation of the ministry and ICBC in the preparation of this report.

ICBC is an integral player in the ministry's database environment because it physically holds the database. The ministry is legally responsible for the database and the policies governing access to it. However, ICBC holds the data in its computers and is responsible for maintaining and updating the database. The rationale is that ICBC is the public body legally responsible for providing vehicle insurance and registration through its network of Autoplan brokers across the province.

This Office, through prior site visits involving the Commissioner and staff members, has developed a working relationship with the ministry and ICBC. Within months of this Office's being established, we visited the ministry site (Motor Vehicle Branch, headed by the

Superintendent of Motor Vehicles) and reviewed its facilities and its legal mandate. Our concerns over potential conflicts between the ministry's data policy and the requirements of the *Freedom of Information and Protection of Privacy Act* resulted in the ministry retaining independent consultants to perform a complete examination of its database and its policies for access to the database by various user groups.

The ministry gave this report to this Office for comment, the result of which was a detailed submission from the Commissioner, which the ministry is now considering as it formulates new policy to govern access. The Commissioner's response outlined the principles established by the *Freedom and Information and Protection of Privacy Act*, which should govern who has access to the personal information in the database and the circumstances under which access should be permitted. We appreciate the co-operative spirit with which the ministry has entered into discussions aimed at enhancing the protection of personal information in its vehicle database.

5. Users of the Motor Vehicle Database ICBC itself makes the greatest use of the Motor Vehicle Database. In addition, Autoplan brokers throughout the province have access through the Vehicle Records Unit at ICBC. Autoplan brokers enter into a detailed written agreement with ICBC, which obligates them to follow the specific requirements of the vehicle registration, licence, and insurance manual.

The Vehicle Records Unit also acts as the gateway for requests by several other classes of users: these include search account holders, parking companies, and municipalities. The parking companies and municipalities each enter into an agreement, referred to as Memorandum of Understanding (MOU), which sets out the terms under which they can obtain access to and use of personal information in the database.

The municipalities rely on access for collecting fines on vehicles under their own bylaws. Parking companies likewise use the information for their system of privately-assessed penalty collection, or for tracing ownership of an occasional abandoned vehicle. The search account holders are most typically represented by law firms, which seek out information about a registered owner in furtherance of personal injury litigation, debt collection, or estate and probate work.

For each separate request for information, account holders are required to state their reason for seeking access to the database. Thus ICBC's Vehicle Records Unit is able to make a determination on the acceptability of each request.

Three other groups of organizations have direct access to the database by means of dedicated data communication lines. (See the general diagram attached as Appendix two.) These include law enforcement agencies, ministries of the province, and registry companies.

Eight registry companies have entered into agreements with the ministry to obtain access to the database for the purpose of serving private sector clients. Registry companies also have access to the alpha fiche described earlier in this report. They serve a wide range of clients, from private citizens making one-time requests, to law firms, land surveyors, retail companies, and lending institutions. Registry companies deal with registration and filing of documents, research, and

information retrieval from virtually all of the public registries in the province, including the corporate registry, the personal property registry, and the Land Title Office.

The registry companies and ministries are both restricted in their use of the database by the terms of their written agreements with the ministry. Law enforcement agencies accessing the database through CPIC are the only agencies which are not specifically governed by a written agreement with the ministry.

We have referred above to some of the uses of motor vehicle data currently authorized under ministry policy. Present ministry policy and the current terms of the standard registry company agreement determine that certain uses are unacceptable:

- making a list of owners of certain vehicle types
- soliciting business
- skip tracing
- a person thinks he/she saw old friend driving a car and wants to contact her
- a car splashes someone, and a person wants his or her cleaning bill paid
- wanting a date
- real estate agent wishes to contact a person seen looking at a house for sale
- traffic disputes--"he was driving like an idiot and cut me off"

While some of these inappropriate purposes may seem benign or even humorous, the fact remains that the acquisition and exploitation of personal information from registration data that must be displayed by law creates an avenue for potentially serious invasions of privacy, which at the least can be annoying and at worst carry potentially fatal consequences.

D. DISCUSSION AND RECOMMENDATIONS

1. Limiting access to the Motor Vehicle Database

It is an unfortunate reality of the 1990s that nasty--though thankfully rare--examples of the consequences of database access can be conjured up, such as women being stalked through information obtained from their license plate data. The consequences, which include harassment and intimidation, are matters of extreme urgency, given the fact that in some cases stalking has ultimately led to murder. In addition, in this and other jurisdictions there have been threats made against individuals engaged in issues or practices which generate controversy. The abortion issue, which has recently focused attention on the database, is a case in point. Labour-management unrest, and conflicts which can lead to personal threats and reprisals, are further examples.

We should make it clear to the reader that the above references to various user groups do not constitute an endorsement by this Office of the current regime for database access. This Office takes the view that private sector, commercial uses of motor vehicle data should be limited to uses which are consistent with the original purpose for which the information was gathered, or which are otherwise allowed under section 33 of the *Freedom of Information and Protection of Privacy Act*. The range of situations in which the database is consulted may have led many

members of the public to believe that it is a public registry, in much the same manner as the Land Title Office is currently regarded. To put it most simply, that is not true.

In addition, this Office has real concerns about the possibility for misuse of the alpha fiche, since it is a non-computerized, self-contained collection of data which will by itself not produce an electronic trail showing when and to whom information has been released. ICBC is concerned that discontinuing use of the alpha fiche by the private sector will increase the number of inquiries received by ICBC's Vehicle Records Unit, with resultant increased administrative costs for that department. While we sympathize with that concern, our primary focus is to ensure data use which is demonstrably responsible, accountable, and consistent with the intent of the *Freedom of Information and Protection of Privacy Act*.

Recommendation 1: **The ministry should limit access to the Motor Vehicle Database to those users whose need to obtain access is consistent with the reason for which the information was gathered in the first instance. The ministry should also examine use of the alpha fiche by the private sector, with emphasis on auditing use of its alpha fiche, and report within three months to this Office its proposed policy for continued or limited access. 2. Written agreements with the Canadian Police Information Centre**

CPIC is an operational database that is used, among other things, to identify or locate persons and property for various police purposes. It is a computerized information storage and retrieval facility designed for the sole use of participating law enforcement agencies on a year-round, 24-hour per day schedule of operations. The system consists of a central automated data bank located in the Royal Canadian Mounted Police (RCMP) complex in Ottawa and linked through a communications network to remote computer terminals across Canada.

CPIC is a shared resource within the Canadian law enforcement community. The quality and effectiveness of this police support system depends on correct user procedures. According to CPIC officials, "the individual terminal operator is the most important link in the entire network with regard to accuracy and relevance of data. The lives of those enforcement officers `on the beat' are best protected by timely, reliable information."

The present CPIC network accommodates approximately 1,500 computer terminals providing direct access to the CPIC database. They are also used for narrative communications with all agencies linked to the network and with other interface systems connected to CPIC. In addition to recording and retrieving data, one agency can send a message directly to another using the communications network set up between all CPIC agencies. Users also have access to foreign information sources through computer systems interfaced with it. Audit teams help to ensure the security of the information and proper terminal use.

At present CPIC users have direct access to the Motor Vehicle Database; they do not have to be routed through a gateway or any intermediate system to extract vehicle and registered owner information from it. There are indeed situations in which an officer's life, or a crime victim's life, may depend on speedy data retrieval; direct database access facilitates this process.

The ministry cannot currently "see" with its electronic audit trail who is sitting behind the CPIC terminal. The cooperation of the police force operating the terminal is necessary to determine who the user was at the time the access to the Database occurred. CPIC access to the Motor Vehicle Database is granted on a "system-wide" basis. The ministry is not granting access to one individual with a terminal (as might be the case for a small insurance office) but rather is granting access to another entire system with all its accompanying terminals.

CPIC is a consistently high volume user of the Motor Vehicle Database and, at present, there is no written agreement between the ministry and CPIC to define the permissible reasons for which CPIC users have access to data. A written agreement is important because it spells out the permitted uses of information and dispels any ambiguity or uncertainty about whether a certain action or use may be appropriate. It certainly provides greater clarity than "unwritten rules," which are apparently what guide CPIC users at present in their use of this database. A written agreement could also act as a baseline for a compliance audit, if the ministry chose to conduct a review of CPIC access to its database.

On a distinctly positive note, this Office is encouraged by the recent policy on access to CPIC data put in place at the Delta Police Department by Chief Constable Cessford. It incorporates some of the "purpose of use" and audit trail principles described in greater detail later in this report. A copy of Delta's new CPIC policy is attached to this report as Appendix three.

Recommendation 2: **Where a written agreement does not exist with a user group, such as CPIC, such an agreement should be created, which will lend substance to what may in the past have been appropriate, but unwritten, rules regarding data access and data use. This agreement should incorporate fair information practices as its foundation, consistent with Part 3 of the *Freedom of Information and Protection of Privacy Act*.**

3. Audit trails

Although increasing public awareness of privacy issues--the main reason for producing this report--is in a developing stage, the field of privacy as a subject for research and writing has existed for at least several decades. In that time, privacy principles have been identified and refined and now form the basis for data protection legislation in all advanced industrial societies. These principles, known as **fair information practices,** have been explicitly incorporated into Part 3 of the *Freedom of Information and Protection of Privacy Act*. The essential principles follow below, with examples of related *Freedom of Information and Protection of Privacy Act* sections provided in brackets:

- Data collection by an agency of government should be explicitly authorized by law (section 26(a)), with a responsible keeper for that information (section 6, and Schedule 1, under definitions of "head" and "public body");
- Personal information, when collected, should relate to, and be necessary for, an operating program or activity of the agency (section 26(c));
- With limited exceptions, an agency collecting personal information should tell the data subject the purpose for collecting the information, the legal authority for collecting it, and

provide detailed information as to who can answer any questions the person may have about the information collection (section 27(2));

- Personal information should be collected directly from the person concerned, unless another method of collection is authorized by the person, or by law. The data subject should be provided with information which will make informed consent possible and meaningful (section 27(1));
- The existence of government data banks should be known; there should be no secret data banks (section 72);
- Personal information collected and maintained should be as accurate as possible (section 28);
- An individual should have complete and unrestricted access to his or her personal information held by government (subject to limited exceptions) and be entitled to request correction of any incorrect information about him or her (sections 4(1), 75(3), and 29);
- Personal information should be used for the purpose for which it was collected, or for a reason consistent with the purpose of collection (section 32(a)). It may be used for other purposes, if the subject of the information consents (section 32(b));
- Personal information may be disclosed by a government agency only as authorized by the data subject by law (this includes the *Freedom of Information and Protection of Privacy* Act, which allows for example, limited disclosure for research purposes--section 35), or to a law enforcement agency for a law enforcement purpose (section 33);
- Individuals have the right to be forgotten: personal information should be kept only as long as needed for a legitimate purpose of the data collector and then destroyed or archived (section 31).

Within the context of privacy protection in the Motor Vehicle Database, the above principles may be condensed to three key elements:

1. **Access to information should be on a "need to know" basis**--Individuals should not be able to access data beyond what is necessary to conduct the searches authorized by written agreement with the ministry;

2. There must be a **chain of accountability** in the system for access to the personal data. The head of a public body should determine responsibility and authority for data access and disclosure, from the level of the terminal operator to the system operator. This is intended to aid compliance investigations and to guard against access by unknown, unauthorized, or casual users, by ensuring that everyone with access to the Motor Vehicle Database has a vested interest in preventing unlawful access and a chain of accountability to a responsible senior official.

3. There must be a means to **audit the auditors**. In practical terms, this means that organizations such as this Office--the Office of the Information and Privacy Commissioner--should have access to the results of a defined audit system. This system should incorporate well-defined procedures and responsibilities which may be examined and tested, to determine whether the audit system is functioning as it should to protect against unauthorized disclosure of personal information.

The key to protecting personal privacy in the present context can be summarized in one word: **auditing** for compliance with fair information practices. Such auditing may have both technological and human elements; that is, auditing capabilities need to be incorporated to a high degree of sophistication in the software which extracts information from the Motor Vehicle Database. Secondly, auditing can refer to a human practice of conducting site visits and physical audits of the records of a company or other entity having access on a continuing basis to the database.

There are therefore two elements to auditing: the power to construct a data trail to follow all instances of access to a database for particular information, and the human capacity to conduct site investigations, which can delve more deeply into the reasons for a particular request.

In each case, the deterrent effect will be the same: users of the Motor Vehicle Database will know in advance that their actions can be electronically traced and may well be randomly audited for compliance in any event. At present, the Motor Vehicle Branch of the Ministry of Transportation and Highways has no personnel dedicated to the conduct of audits for compliance with the terms of agreements that users enter into with the ministry.

Recommendation 3:

The Ministry of Transportation and Highways should establish an audit program for compliance with fair information practices with individuals trained and assigned to the specific task of conducting audits of the Motor Vehicle Database user group community.

Example: Auditing in Action for Automated Patient Records

In March, 1995, a Vancouver radio station reported that several staff at the Royal Columbian Hospital in New Westminster had been inappropriately accessing certain patient files. The hospital's security task force had discovered the inappropriate access through a special audit trail of access by staff to the records of high-profile patients and of hospital staff who were patients. The hospital's computer system provides a clear record of who has had access and when. The security committee was able to determine who had accessed the record in the course of their staff duties and who had been "browsing." As a result of the audit, the hospital is reviewing the levels of access granted to various categories of staff. In addition, as part of a larger hospital-wide educational approach, the screens of the computer system feature messages advising users that usage of the system is being audited on a regular basis. These messages appear at random on screens.

---

4. Adequate software

At present, ICBC has the capacity to conduct electronic audits by scanning information "transactions" involving access to the Motor Vehicle Database. However, the process is

cumbersome and extremely labour intensive. The information obtained from a search must be analyzed to determine whether each episode made sense and is justifiable from a business perspective. The assistance of the registered owner of a vehicle might be necessary to make sense of a particular request and determine whether it was made for a legitimate purpose, such as an application for a loan or a renewal of insurance.

The Data Security section at ICBC is currently working with ICBC's Information and Privacy department to place a specific classification on all forms of accessed data to indicate how the data may be used. The Data Security section is also working on a project to match access privileges to the job function an employee performs. This is a practical application of the "need-to-know" principle.

Internal Audit, Data Security, Claims Operational Systems, and the Application Engineering--Corporate sections of ICBC have together been assigned the task of investigating "suspicious" access to corporate data via the on-line system. This function is currently being turned over to the Freedom of Information department. While all accesses logged by the current system are "authorized" in some fashion, not all accesses may be lawful or appropriate.

ICBC has made significant progress over the past five years in modernizing its database, tightening security, and providing audit trails. Yet, because the database has its roots in earlier technology, it lacks the power and flexibility to generate quick, thorough electronic audits. Such capability is essential, if ICBC and the ministry are going to be able to protect the integrity of personal information in the Motor Vehicle Database and respond to the legitimate expectations of confidentiality of its customers.

ICBC should also pursue a means to provide registered owners who have special privacy risks with a way to limit electronic access to their personal information. However, this Office acknowledges the magnitude of such a task from a technical, financial, and policy viewpoint. To create different levels of accessibility for classes of personal information, in much the same manner as an unlisted telephone number, poses major challenges for database designers and policy makers. This Office will revisit this general issue in the future, particularly in the context of providing privacy protection for those individuals--some of whom are employed in the area of justice and law enforcement, for example--whose responsibility or visibility or life experience makes them vulnerable

Recommendation 4: **The software employed by ICBC for the Motor Vehicle Database should be re-engineered so that there is a powerful, easily accessible electronic record of all entries into, and output from, the database, including a record of the number of and type of files consulted.**

5. Internal privacy codes

Users of the Motor Vehicle Database understand that their access to information is specifically limited by the terms of the agreement they enter into with the ministry. However, it is apparent to this Office that the consequences for violating those terms may not be sufficiently clear, or negative in character, adequately to deter improper use of the personal information gained.

Guidance for user groups should come from internally-created **privacy codes** that incorporate appropriate fair information practices. These are declarations which set out standards which identify for all the members of the user group what information is being accessed and used, why it is important to respect the rights of the information subjects, and how those rights can be respected. At present, privacy codes are used in many areas where legislation does not yet apply, as a means of demonstrating to the public that information users take privacy rights seriously.

The Canadian Standards Association has consulted widely toward this end and is at present working toward approval of a detailed model privacy code with wide potential application in the private sector. This proposed model code incorporates and in some cases amplifies the principles of fair information practices outlined earlier in this report. These principles are provided in summary form in Appendix three to this report.

Recommendation 5: **The terms of future agreements with Motor Vehicle Database users and registry companies should be more rigorous and should specify that non-compliance with the access policy constitutes a fundamental breach of the contract. In addition, all user groups should be required to create and adopt their own privacy codes which will bind all members of the user groups. The privacy codes must have substance, be meaningful, and incorporate the basic principles of privacy protection identified in this report.**

6. Public education

It is an ancient maxim of law that "the law does not protect those who sleep on their rights." In order for individuals to enjoy the best protection of their personal information, it is important that they understand what personal information is and what rights they enjoy with respect to keeping that information personal. Public education and the enforcement of the rights conferred by the *Freedom of Information and Protection of Privacy Act* are two of the fundamental reasons for the establishment of this Office. If individuals understand that certain uses of their personal information are unlawful, and know who to complain to in such an event, an informed public will likely prove to be the most effective deterrent to information abuse.

Recommendation 6: **ICBC, in collaboration with the ministry, should embark on a public education project aimed at informing vehicle registrants of their privacy rights under the *Freedom of Information and Protection of Privacy Act*. The information contained should spell out in clear, understandable language the avenues for launching privacy-related complaints, both within ICBC or the ministry, and to the Office of the Information and Privacy Commissioner.**

E. CONCLUSION: STEPS FORWARD

This report is an example of how the Office of the Information and Privacy Commissioner is attempting to heighten public awareness of individual privacy rights and the privacy risks associated with common commercial transactions and database technology. Implementation of the recommendations contained in this report will assist in protecting the public, but only if the public is aware that certain uses of personal information are inappropriate, and that they have a right to object to, and demand the investigation of, any inappropriate use. Each British

Columbian should thus act as his or her own privacy watchdog. It is in that spirit and with that sincere hope that this report is released.

ICBC and the ministry are together commencing a number of initiatives aimed at providing greater protection for personal information held in the Motor Vehicle Database. These current initiatives include:

- A review of the legal rights of current external users to information and their need for access--in other words, a detailed examination of the "need to know" principle which is at the heart of any adequate policy on access to a database;
- Tightening the language of Memoranda of Understanding and other legal documentation, consistent with the intent of recommendation 3 listed above;
- Generic identification for access terminals will be progressively eliminated to ensure against access by an otherwise "anonymous" user;
- Insistence on expiring passwords, that is, passwords that will have to be continually updated in order to ensure access to the system;
- Further training and instructions to users to heighten awareness of the critical privacy issues involved with access to a database;
- Improvements to the DART system are being considered (this is the **D**irect **A**ccess **R**equest **T**racking system used to grant access to the database);
- A review of non-transactional access to information, for example by programmers, is being undertaken;
- A data classification process has begun whereby data are classified according to the degree that they are personal or confidential; this in turn will be matched with various levels of data access on a "need to know" principle; and,
- optical disk technology will be explored for the storage of audit tape records; this would provide both greater storage capacity and greater ease of retrieval when an audit is conducted.

The data administration section at Motor Vehicle Branch has recently articulated a policy of protecting the confidentiality, integrity, and, where appropriate, the availability of data by ensuring that: a) Every subject area has an identified data owner; b) Usage of Motor Vehicle Branch data complies with the *Freedom of Information and Protection of Privacy Act*; and, c) Use of or access to Motor Vehicle Branch data, inside or outside Motor Vehicle Branch, must adhere to specific stated procedures.

David H. Flaherty
Information and Privacy Commissioner
Victoria, British Columbia
March 31, 1995

Investigation conducted by Michael T. Skinner
Report written by Michael T. Skinner
Additional material by R. Kyle Friesen

January 6, 1995

Investigation of Possible Inappropriate Access to Personal Information from the Motor Vehicle Branch Vehicle Registry

The Office of the Information and Privacy Commissioner of British Columbia will commence an investigation of alleged inappropriate access to personal information from the Motor Vehicle Branch vehicle registry. Media reports on January 5, 1995 indicate that someone at the Delta Police department allegedly accessed personal information from the MVB registry, specifically names and addresses of volunteers and staff of Everywoman's Health Centre.

Terms of Reference

1. The Office of the Information and Privacy Commissioner, under section 42(2) of the *Freedom of Information and Protection of Privacy Act*, will investigate the alleged improper access to personal information. The Delta Police Department, as a municipal police force, the Insurance Corporation of British Columbia (ICBC), and the Superintendent of Motor Vehicles in the Ministry of Transportation and Highways are all public bodies subject to the jurisdiction of the Act.
2. The Commissioner's concern is with the general problem of third party access to widely-used data bases, such as the Motor Vehicle Branch vehicle registry. A secondary concern is the possible inappropriate use of the Motor Vehicle Branch vehicle registry by those with access to the Canadian Police Information Centre (CPIC) computer system.
3. The Commissioner's investigation is independent of other investigations by the RCMP, the Delta Police Department, and ICBC, because of its focus on the access, privacy, and security provisions of the *Freedom of information and Protection of Privacy Act*.
4. This investigation will result in a public report. The speed of our inquiry will depend, in part, on how quickly we can access relevant materials compiled by other investigators.
5. The specific focus of our inquiry will be measures that can be taken to protect the privacy of individuals whose information appear in data bases that are accessible to multiple parties.
6. All interested parties have been notified in advance of this investigation, including the Attorney General, ICBC, Delta Police, and the Superintendent of Motor Vehicles.
7. These terms of reference do not necessarily limit the scope or mandate of our investigation.

For more information, contact:

Pamela E. Smith, Research and Communications Officer
Office of the Information and Privacy Commissioner
(250) 387-5629

APPENDIX ONE

APPENDIX TWO

ADMINISTRATIVE BULLETIN #95
Approved: 95-02-23

J. Cessford
Chief Constable

CANADIAN POLICE INFORMATION CENTRE - CPlC

The following policy will be added to the Administrative Manual at the next revision. The Canadian Police Information Centre (CPIC) is a computer system provided by the Solicitor General of Canada to all police agencies in Canada.

CPIC operations are governed by the CPIC Operations Manual and usage of the system will be conducted with strict compliance both the CPlC Manual and the Delta Police Policy and Procedure.

ACCESS TO CPIC DATA

The Chief Constable is responsible for adherence to CPIC Operational policy and authorizing access to CPIC data.

All CPIC information is to be considered confidential and will only be provided to a person(s) who are authorized to receive the information and has signed an oath of confidentiality.

Only those members who have had CPIC training are authorized to conduct queries of the CPIC system.

All queries of the CPIC system will contain the identity of the member requesting and the location of the query.

All hit confirmations and narrative messages will contain the identity of the originator.

AUTHORIZED RECEIVERS OF CPlC DATA

The Chief Constable is the CPIC Authority within the Delta Police Department. Only persons who come under the control or authority of the Chief Constable and have taken an oath of confidentiality, may be provided with CPIC information. Other police members or peace officers who are conducting an investigation in Delta will also be provided with CPIC information. Any information released will only be provided for police purposes.

APPENDIX THREE

CPIC data relating to the prosecution of an individual(s) will be provided to Crown Counsel.

RELEASE OF CPIC HARD COPY

All CPIC hard copy will be routed to the file, individual or department to which it relates. The receiver of the hard copy will be responsible for the security of the material. All CPIC hard copy created for routine operations and maintenance will be shredded daily.

All CPIC hard copy which exist in operational files will be maintained in an orderly fashion. Routine requests for files containing CPIC hard copy will be reviewed and all CPIC hard copy will be removed prior to responding.

Files containing CPIC hard copy to which an application under the Freedom of Information and Protection of Privacy Act is received will be altered by removing the header format only. Other information on the hard copy will be reviewed having regard to the personal privacy of individuals.

A Judicial Order for a certified true copy of a record or file which contains CPIC hard copy will not be altered.

Model Code for the Protection of Personal Information

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. **Accountability** An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.

2. **Identifying Purposes** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information except where inappropriate.
4. **Limiting Collection** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention** Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
6. **Accuracy** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness** An organization shall make readily available to individuals specific information about its policies and practices relating to its handling of personal information.
9. **Individual Access** Upon request, an individual shall be informed of the existence, use and disclosure of personal information about the individual and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance** An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

December 1994

APPENDIX FOUR