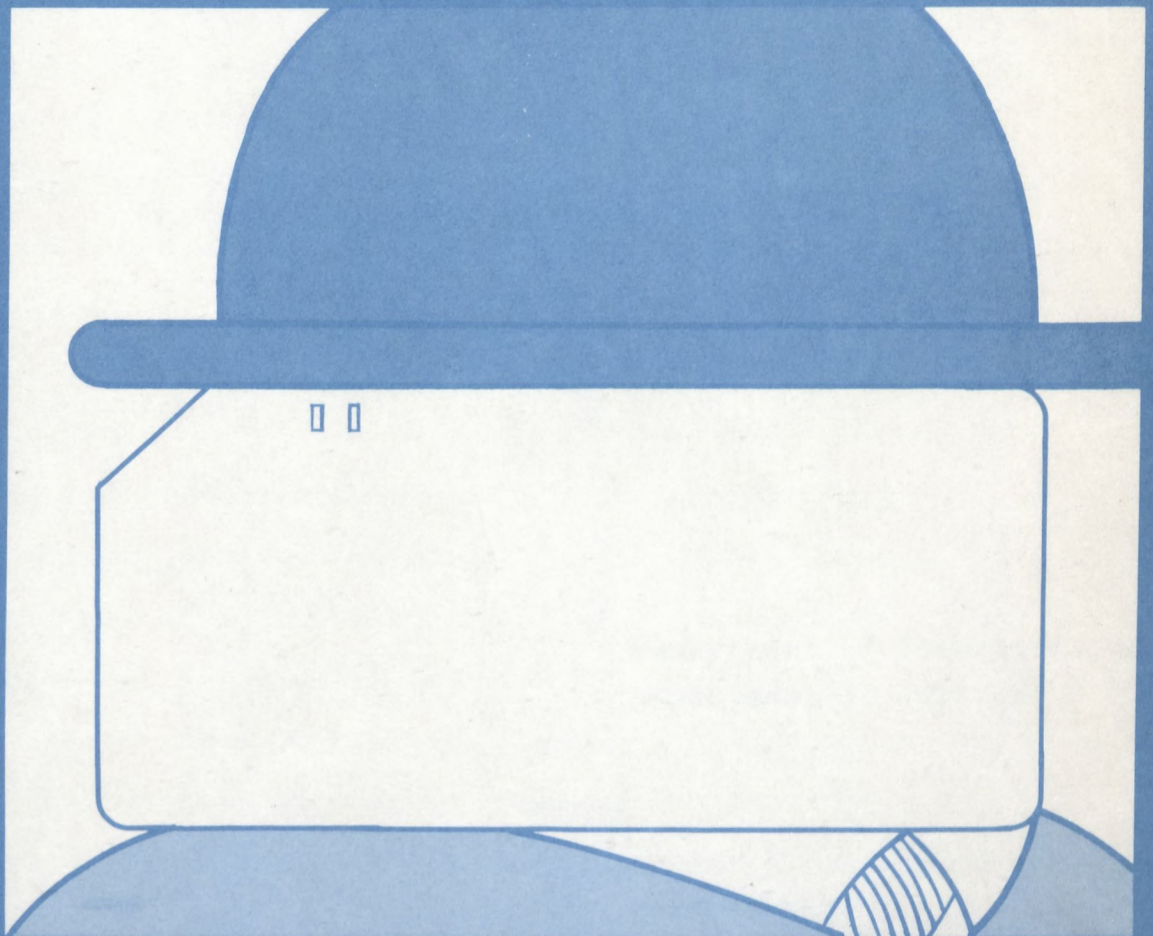


QA
76.5
.C352
[no. 6]

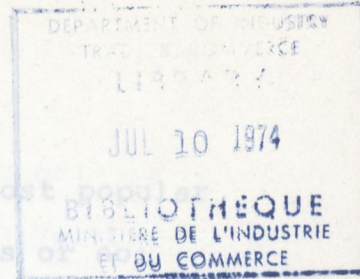
REGULATION OF FEDERAL DATA BANKS

K. KATZ



6 A study by the Privacy and Computer Task Force

Preface



Personal privacy has become one of the most popular topics for study by governments in the last 5 years or indeed, there is hardly a developed country that has not, either directly, or by means of participation in international undertakings, looked at this subject intensively with a view to strengthening it under the law. Countries which have demonstrated concern for privacy are those which are both technologically advanced and which have a constitutional tradition of libertarianism -- the western European nations, Canada, and the United States in particular. The Privacy and Computers Task Force represents the major Canadian undertaking in this field.

REGULATION OF FEDERAL

DATA BANKS

A STUDY FOR THE

PRIVACY AND COMPUTERS TASK FORCE

The concern for the value of individual privacy at this time comes from an awareness of the possibility of its erosion by force of technological change and innovation, particularly as it relates to the context of personal information, one of the three universes of personal privacy identified by the Task Force. The computer has become the focal point, for its ability to store, process, and disseminate massive amounts of information has generated a set of concerns about the effects of information flow on privacy that had not previously been viewed as a cause for alarm when information processing had been exclusively a manual affair.

Department of Communications
Department of Justice

KENNETH KATZ

Preface

Personal privacy has become one of the most popular topics for study by governments in the last 5 years or so; indeed, there is hardly a developed country that has not, either directly, or by means of participation in international undertakings, looked at this subject intensively with a view to strengthening it under the law. The countries which have demonstrated concern for individual privacy are those which are both technologically advanced and which have a constitutional tradition of libertarianism -- the western European nations, Canada, and the United States in particular. The Privacy and Computers Task Force represents the major Canadian undertaking in this field.

The concern for the value of individual privacy at this time comes from an awareness of the possibility of its erosion by force of technological change and innovation, particularly as it relates to the context of personal information, one of the three universes of personal privacy identified by the Task Force. The computer has become the local point, for its ability to store, process, and disseminate massive amounts of information has generated a set of concerns about the effects of information flow on privacy that had not previously been viewed as a cause for alarm when information processing had been exclusively a manual affair.

The computer has had the effect of taking privacy investigation backwards to examine the relationship between personal information and privacy without regard to the manipulatory techniques. It has also focused on the data collectors. It is in this light that the Task Force has undertaken to look at personal information systems within the federal government, the biggest data collector and information repository in Canada. This particular study will examine data collection and storage policies and practices of the federal government, and look at some of the ways and means available for controlling these practices for the sake of minimizing the deleterious impact on individual privacy they potentially afford.

Chapter One

Classification of Government Records and Systems

In the information context, three potentially intrusive elements exist, these being (a) information accumulation practices, (b) information storage techniques, and, (c) information dissemination policies. Of these three, the first element has been excluded from the terms of the Task Force, not because the accumulation of data does not constitute potential invasions of privacy, but rather (as will be shown) because the central issue is the use made of information, no matter how much and in what manner it is collected. The area under examination is thus restricted to data storage and dissemination, both of which produce a distinguishable series of threats to the privacy of individuals.

The privacy problem in the information context is not unique to a machine environment. The computer only exacerbates what remains fundamentally a political issue. Individual privacy, as well as other fundamental rights which privacy may protect, is a function of an individual's ability to control the extent to which personally identifiable information will be spread. Information extracted by governments and stored in data banks can be put to secondary and tertiary uses without the knowledge of the subject, and can react upon that individual affecting his rights, privileges, status and opportunities. The traditional balance between government and citizen may shift markedly in favour of

government when, by means of manipulation of the information it maintains on its subjects, the state can create a comprehensive profile of the subject far beyond the primary data it has gathered. In its most extreme form, the privacy threat may emerge from a new, more effective surveillance and production capability on the part of government. The private lives of individuals, the characteristics which distinguish one man from another, become data by which the individual is identified to the power structure. As compulsory disclosure of personal characteristics increases, the ability to withdraw into anonymity diminishes.

Information systems (or data banks, ⁽¹⁾ as they are now called) containing personal data about individuals have been maintained by both the state and private organizations since the beginning of civilization. ⁽²⁾ Until recently, these records about individuals were kept in manual form and in separate filing systems. The ability to aggregate separate records about the same person depended on a cross-indexing system, as well as physical access to the various locations where files were kept. The procedure was difficult, time consuming, and not very common. Information accumulation and file or record integration, which could threaten individual privacy, was thus only hypothetical.

Computerization, on the other hand, especially when coupled with integrated computer-to-computer communications systems, has transformed this inchoate threat to individual privacy

into a real one: Computerization not only results in high speed multi-file access, but because of the virtually limitless amounts of information which the computer can store in one place and retrieve instantaneously, it induces an increase in the propensity to acquire data.

The threat to privacy does not now lie multi-purpose data banks maintained by the federal government. Few if any of these exist. Rather, individual privacy is made vulnerable by access to, and dissemination of, personally identifiable information maintained in at least fifty discrete locations. They can isolate individuals possessing any of the following characteristics:

(3)

1. racial background
2. religious preference or practice
3. marital habits
4. reputation in the community
5. character references
6. recreational habits
7. political practices
8. medical history
9. educational background
10. membership in clubs and associations
11. results of personal or psychological tests
12. income
13. employment history
14. investments
15. paying habits, including outstanding credit obligations and cost of living obligations

These personal references may be located in more than one record system, since no significant centralization of records is underway. Hence record content alone will not furnish an adequate means of distinguishing among various government systems. An individual's employment record, for example, may be located in such systems as those of Canada Pension Plan, National Health and Welfare or National Revenue, as well as a variety of other agencies. In some cases the contents of an individual's file will be quite similar in totally separate systems, although the use to which the information is put may be radically different.

The information itself is the data base; the system which controls the data base is the data bank. Neither autonomously can impact upon privacy. Once it has been determined that a particular file contains information which is personal and which will occasion a loss of privacy upon disclosure, the purpose for which that information was collected will become the only effective basis upon which classification of government systems for regulatory purposes can be established.

A basic output distinction at the file (or single-purpose system) level may be drawn between those files which are operative and those which are non-operative with respect to individuals. The non-operative category include files maintained for internal administrative uses and for statistical

purposes.⁽⁴⁾ The operative files are those which are established by reason of some kind of government exchange with individuals where the processes of inserting, updating, reporting, or deleting the record of a private citizen are accomplished for the sake of making a determination ultimately affecting the interests of that very subject. In a sense all operative files are regulatory in nature, but these have been divided into the administrative file and the intelligence file. The relevant files in government systems are the statistical file, the administrative file, and the intelligence file.

1. Statistical Files

The statistical file or system is organized to receive and collect data on individuals or groups in order to study statistical variations in the characteristics of groups. Although such systems require identification of the data as to individuals in the sample populations for specific purposes (such as longitudinal studies), data on individual persons are not their intended output. Where the particular information which generates the statistic is itself not disclosed and the aggregates cannot be broken down so that individualized extrapolation becomes possible, this category is not considered threatening to individual privacy.

2. Administrative Files

These files are deliberately organized to furnish reports about specific individuals, reports which will be used to make judgements affecting individuals' rights, benefits,

status and opportunities. Since individuals are identified in terms of personal information, these files pose serious threats to personal privacy and should be the focus of regulatory concern, as regards storage of information and access to it.

3. Intelligence Files

These files are of the same nature as administrative files, in that they are operative and they affect the individuals' rights, benefits, status, and opportunities. They encompass files maintained for specific purposes, and are located in the hands of law enforcement institutions and the military. They have been distinguished from the administrative files on the basis of particular interests which must be taken into account in any discussion of regulation. Their content is highly sensitive and usually derogatory. In this sense they may pose the single greatest threat to personal privacy within all government systems.

The specific agency of the government having custody of an administrative or statistical file will not affect the magnitude of a potential privacy violation in the event of its improper disclosure. Rather, it is the content of such a file which will bear a direct relation to the extent of a possible privacy violation.

4. To Recapitulate

Release of employment history, for example usually is regarded as being less serious than release of medical information. Furthermore, disclosure of identical information can be more damaging in one context than in another. Disclosure of a name and address by a motor vehicle licensing bureau, for example, cannot be considered equivalent to dissemination of a particular name in the context of a list of mental health patients or welfare recipients.

The ultimate harm that may result in consequence of a violation of privacy that occurs in each case may be different, even though the direct result, the loss of privacy, is the same. Unless ultimate harm stemming from a breach is calculated, or inherent sensitivity levels of all personal information are developed, distinctions in depths or degrees of privacy will remain largely subjective.

Chapter Two

Regulation of Government Systems

a) Statistical Systems

1. Privacy Controls

As was stated earlier, the threat to privacy posed by statistical systems is a function of storage techniques and statistical methodology adopted. Pure statistical systems which yield no personalized information are not potentially harmful to privacy in terms of their output.

The primary operation in statistical development, apart from the actual data gathering, is the compilation of the information collected. The accumulated results comprise the raw data, the basis for any statistical tabulations. The raw data may produce a serious threat to privacy if released in this form, since the personal reference points are still aligned to the personal identifiers. In effect, individual records exist for every respondent which identify him in terms of the characteristics assembled.

If the exclusive purpose of the collection is statistical, the data gathered does not have to be stored in this raw state. It immediately can be compiled, the identifiers removed, and the

basic statistical units created. At this point the threat to privacy will have been largely obviated. As long as the basic statistical units are not so small that individual identification can be derived by means of extrapolation and cross-referencing, penetration of the system will not yield individualized results and will not permit a breach of privacy. Once the primary aggregates have been assembled, the raw data itself (e.g. completed questionnaires) no longer need be kept.

A list of four rules which, with appropriate adaptations, can serve to assure a minimum level of privacy protections in statistical systems at large:

- i) The accumulated raw data should not be filed (or recorded) in that state.
- ii) The raw data should be compiled into aggregates as quickly as possible upon receipt.
- iii) Once aggregated, the raw data should be destroyed. This requirement, however, cannot be absolute. Where statistical operations are continuous, the basic data cells will not themselves meet an evolutionary need for new statistical tabulation in a different format from the original one. In those cases where raw data must be stored, the fourth rule in this list would apply.

or

- iii)(a) Consideration might be given to actually returning completed questionnaires to respondents. This might develop public trust of census-like operations and would result in removal of the raw data as well. A prohibition against duplication of completed questionnaires would be required to make the obligation of returning them meaningful.
- iv) Where data accumulation serves other than exclusively statistical purposes, requiring that raw files be maintained, these files should be stored in a location completely separate from the statistical files.

2. Application to Government Operations

Within the federal government, the great majority of statistical files and systems dealing with personal information is located within one department, Statistics Canada. It alone conducts decennial and periodic census, and carries out statistical surveys required by government. Its officers are governed by a statutory obligation of secrecy with respect to accumulated raw data.⁽⁵⁾ Statistics Canada is obligated to format its tabulations so that individual identity may not be derived from the aggregates it publishes.⁽⁶⁾ The Statistics Act provides penalties for infringement of these rules.

In other departments and agencies there may exist statistical files, either based upon operative data or assembled for a particular task of a department. Furthermore, specific federal projects, such as the Privacy and Computers Task Force, will require surveys and statistical tabulations. In none of these cases is there a statutory obligation of secrecy, notwithstanding promises of confidentiality that may have been given to respondents at the outset. Neither will an obligation equivalent to that in s.15(2) of the Statistics Act apply.

In these instances, the relevant agency could be governed in one of two ways for privacy's sake: either it could be obliged

to engage Statistics Canada to conduct the survey, subject to the rules in the Act, or it could be made subject to the Act itself for the purposes of the survey. In the latter case, the promise of confidentiality would be enforceable. If neither alternative can be applied, then the general controls regarding storage of raw data and statistical tabulation formulated above should apply. If raw files must be maintained, they should be governed as though they were operative administrative records. If a promise of confidentiality is actually held out to respondents, a breach thereof could be made actionable per se, in which case the necessity of proving harm will be removed.

The major reason for differentiating statistical systems lies in the degree of protection required for systems security. Since statistical systems as such will not yield individualized results upon penetration, the amount of hardware and software required to protect them is considerably less than in operative systems where the threat to privacy following intrusion is high. Economic considerations relate to systems security and must weigh heavily in terms of actual threats. For this reason, it has been suggested that total separation between statistical and operative files and systems be established, whereby those files that require protection will be duly secured and those that do not will waste security facilities.

b) Intelligence Files and Systems

1. Nature

For present purposes, these systems or files will be defined as those containing personal information which describes or refers to an individual in terms of characteristics of primary interest to law enforcement or national security agencies. They typically contain criminal histories and security classifications respecting job roles.

In the larger context, these files and systems are administrative in that they contain personal information and are used to make decisions affecting file subjects. They have been separated from the general administrative category because of their particular nature. They may very well contain the most socially sensitive information available. One's personal criminal history is socially derogatory, carrying with it the scarlet letter of moral turpitude. Furthermore, these files have been isolated because of the need to take account of certain extraneous factors which must influence their regulation.

The decisions taken on the basis of accumulated intelligence data differ radically in terms of the effects they portend for the subject. The very reason for data accumulation in the first place is different, since the focus is not on the protection and security of the individual, but of society in

general. In most cases, the individual subject is affected negatively, since the information collected and stored in these systems is largely derogatory. Privacy is not the only interest at stake in this context; abuse of these records may engender far more damaging consequences to the individual. For these and other unstated but similar reasons, such records require particular attention. Since police forces are the main collectors and handlers of such data, the criminal history information will be regarded as comprising the greater part of these records in general, as the main undertaking of any police force is law enforcement.

2. Location and Content

Criminal law enforcement in Canada is subject to a curious blend of jurisdictions. While criminal law itself is exclusively with federal legislative jurisdiction,⁽⁷⁾ the over-all administration of justice, which includes prosecutions under the Criminal Code, is assigned to the provinces. Law enforcement outside organized municipalities falls to the R.C.M.P. under contract to provincial governments, except in Ontario and Quebec which have a provincial police force. These officers are agents of the Crown Federal with respect to violations of the Criminal Code. In other cases, such as highway offences, police officers are agents of the Crown Provincial. Furthermore, the R.C.M.P. have exclusive jurisdiction with respect to federal

statutory offences, such as drug violations, notwithstanding the ability of any peace officer to make an arrest. Finally, the R.C.M.P., as agents of the Crown Federal, police the Northwest Territories and the Yukon. Apart from all this, there are special military police for Armed Forces personnel and bases, both in Canada and overseas.

It is thus virtually impossible to determine what specific criminal records will be maintained by the R.C.M.P., where they will be located, whether duplicate files will be maintained by other police forces, or whether duplicates of the originals in the hands of local or provincial police will be given to the R.C.M.P. For present purposes, it is assumed that the overwhelming bulk of police records are maintained at the local level. The present focus of concentration on the R.C.M.P. stems from its capacity to develop a central criminal repository for all criminal histories in Canada. It could conceivably become a clearinghouse for all inquiries from the provinces, as well as foreign states by way of its affiliations to international organizations, such as Interpol.

Preliminary plans to create a criminal history data bank were announced in the middle of 1971. When this fully automated system, with total accessibility from all the provinces on a dial-up or dedicated basis becomes operational, the hardware

and software security devices that will become necessary to protect against intrusion will be considerable. Already various devices exist; specific police terminals are being marketed, and together with encoding techniques for data communications and storage, user and terminal identification routines, physical security, and so on, these systems can attain the highest security level that may be purchased.

3. Privacy Risks

It is possible that police will not divulge personal criminal information to third parties unless required for arrest or prosecution by another police force. Although privacy may be at stake here, what must also be considered is proper law enforcement. The individual's right to privacy must be measured against the need for prosecution of offenders. There is hardly sufficient excuse for blocking liaison between co-operating police forces. This observation, however, is not intended to relate to inherently privacy-intrusive data collection practices, such as wiretapping, eavesdropping and the use of informers. It is only suggested that when information useful in finding a suspect or prosecuting him exists in the hands of one police force, a claim to privacy is not to prohibit the communication of that information to the second police force.

The extent of the data held in police systems has been kept most secret from the general public. The criminal

histories of individuals probably contain such information as previous arrests and convictions, fingerprints, mug shots, known associates and modi operandi.

A question arises as to the legal nature of this information. Previous convictions are part of the public record; they are admissible evidence in criminal proceedings under the Canada Evidence Act. Even though personal, this information is in the public domain. These records are available to Crown prosecutors, attorneys, and, to some extent, to the public. Arrests and convictions (except of minors) are reported in the press, and one has only to leaf through any volume of criminal law reports to become acquainted with the arrest and trial of numerous defendants. Any control on dissemination of this information would require total re-appraisal of the premise, basic to our system of criminal justice, that publicity is to be afforded such matters to guarantee the equitable operation of the legal system.

4. Controls

If controls on government personal information systems, both manual and automated, are to encompass federal police systems, some leeway with respect to the latter will be required. There must be recognition of a special police interest in maintaining security if only to ensure efficient police administration and law enforcement. Similarly, a general protocol

governing dissemination would have to allow for police co-operation in the apprehension and prosecution of offenders, for admissibility of evidence of previous convictions and for the public disclosure of court records. In other cases, additional control over access and dissemination to third parties will be unnecessary, as will special security standards. If the experience of Task Force investigators be at all indicative, R.C.M.P. authorities may well be the most concerned parties in Canada, as regards protecting information in their data systems - and, indeed, general information about the systems - from public knowledge.

An ironic regulatory situation arises with respect to police systems. Unless access and dissemination rules are formulated deliberately to obstruct police co-operation, police systems will normally exceed safeguard standards and prove to represent (in this context) the smallest threat to privacy. The more appropriate focus for regulation of police information systems would appear to be in respect to their data collection practices - creating rules regarding how and what data may be collected, from whom, and how long it may be stored. The impact of these regulations upon the admissibility of evidence in court would have to be considered.

Under this title, one exception worth noting affects personal file access for purposes of verification. A police

file is not established through the initiative of the subject and does not serve its subject in any immediate sense. A particular administrative file might be subject to verifications, so that refusal to provide a benefit will not be predicated on erroneous information. The police file would require similar verification so that a prosecution is not brought on erroneous facts. Even if some legal remedies are available for false arrest and detention, the prosecution cost and time involved, as well as the subject's obligation to prove his case beyond a reasonable doubt (if the remedy be criminal), makes legal redress ineffective in a majority of cases.

Notwithstanding these factors, a right of access for verification may be useful even if privacy itself is not necessarily served by it. One such system permitting access has been established by project SEARCH⁽⁸⁾, which has been described as:

"...an on-line system designed to give state and local police departments quicker access to criminal histories. ...it consists essentially of a computerized central index, plus individual criminal history files and user terminals located in each of the several participating states. The index is queried when a police officer brings a suspect to the station. Name, age and other identifying information is input through a terminal and passed against the index. If the index contains a matching reference, the officer gets back a message telling him which state has the corresponding criminal history. Then, via teletype, he can request and obtain, a copy of the record."⁽⁹⁾

The announced plan for SEARCH permitted system access by subjects to guarantee accuracy of the data in the files held in the central index. The plan also provided for data classification procedures, system audit and the purging of inaccurate, unverifiable and out-of-date information. The SEARCH system, which became operational in November 1971 could be a model for equivalent systems in Canada.

c) Administrative Files and Systems

1. Nature and Extent

Administrative systems and files have been defined as those containing personal information organized so as to produce reports about specific individuals which will be used in determining their rights, benefits, status and opportunities. They may be located in any of the various federal departments, agencies and Crown corporations. In some cases they are redundant and not terribly well-secured. For the most part they are not subject to controls. In many instances, these files and systems have been automated, while others remain manual and subject to various plans for future computerization. No plans have been announced by the government to centralize all records or create access links between the separate systems, although proposals have been advanced for a partial merging of some systems which contain similar information in similar file formats.

Administrative systems and files will contain, for example, personal data upon which eligibility for government assistance is based. They will contain information upon which income and other taxes will be levied, as well as medical information, employment histories, family and education records, and a host of other data, the bulk of which is vital for the operation of federal programs affecting individuals directly. There are even cases, particularly as regards Indians and Eskimos, where virtually complete life profiles may exist.

The "disc" numbers, until recently assigned to all Canadian Eskimos at birth, never were used as comprehensive single identifying numbers ("SIN") around which life dossiers are built. Even the assigning of such numbers has been terminated, with the completion of "Project Surname" by the Northwest Territories Administration.

The total accumulation of federal records, paralleled by similar accumulation at the provincial and local levels, is the product of unimpeded growth in record building. The data accumulators never paused to examine the possibility of rationalizing the multitude of systems that have been created. Limitations on data accumulation would have been the obvious place to start.

2. Impact on Privacy

Taken as a whole, administrative files and systems encompass threats to individual privacy in a number of dimensions. Because these records are operational, the impact on privacy is at first measurable in terms of the actual accumulation of the information itself. To a great extent, they contain information relevant to eligibility criteria established for benefits to which the individual is entitled by law if he meets the stated legal requirements. Where information sought does not relate to eligibility criteria, the statutory power to seek personal information may, in some of these cases, become a licence to violate the privacy of the individual seeking the benefit.

Intrusiveness is a function of the criteria established for determining eligibility, and questions in relation to these criteria are not the principal source of the problem. If it may be assumed that only pertinent information will be sought, privacy resolution will require re-examination of the statutory or regulatory grounds for decision-making in this particular context. The issue becomes one of greater social policy⁽¹⁰⁾.

The access to and dissemination of the information collected represent the principal sources of potential risks to privacy in administrative systems. With the exception of tax records, no explicit statutory safeguards exist for administrative files. The risk posed by unauthorized penetration of a file or

system can be countered at the technical and procedural level. For manual systems, physical security, proper identification, and adequate supervision are some of the means to prevent illegitimate access to records. Automated systems can be secured by such hardware and software devices as user and terminal identification, encoding, threat monitoring and alarm systems⁽¹¹⁾. With proper supervisory methods and enough security built in, unauthorized penetration of the computerized file can cease to be a hazard to the privacy of individuals. Ultimately, the security of a system depends upon the price its operator is willing to pay for sophisticated safeguards.

Once the legitimacy of given data accumulation functions of government has been accepted in an advanced "post-industrial" society such as ours, one is faced with evaluating the risks posed to the privacy of the subject through the dissemination and exchange of this data. To assess the magnitude of this risk in any given circumstance the following questions may be posed usefully:

- who, other than the gathering department, agency, or branch (hereinafter referred to as the "unit") may see the information, and under what conditions?
- must the subject be notified in advance?
- must the subject consent?
- should restrictions be placed at the individual file level?

Merely in answering such questions the extent of the privacy threat posed by any given data system will become evident.

While the terms of reference of the Privacy and Computers Task Force precluded such in-depth examination of each and every federal department, the information necessary to make such evaluations of the various systems appears to be readily available - with the singular exception of systems under the control of the Royal Canadian Mounted Police.

The privacy of the subject is compromised whenever a personal reference characteristic, such as income, is communicated to a third party who can link the reference to the subject's identity, or who is given both the reference and an identifier. Loss of privacy is a consequence of the act of disclosure, even if specific harm accrues only later on - or never at all. Hence, the focal point of this discussion is the loss of privacy itself, rather than whatever harm may result. Preventing the former will obviate any need even to consider the latter.

The question of dispersal of information may be broken down into distribution within government and dispersal outside. In the latter case, a clear prohibition could be set up, one that would put an end to the practice of actually selling lists of names and addresses (as well as other information) to private parties for their commercial operations. Where the file subject's identity is made known to the third party, his privacy clearly will have been breached, notwithstanding the seemingly innocuous result of receiving unsolicited mail. Alternatively, distribution

of names could be confined to subjects who have consented to have their names disclosed. The consent might be solicited by means of having respondents mark "yes" or "no" on the original solicitation or application form. In the practice of selling names, the individual is unable to control at all the extent to which his identity becomes known, particularly as these lists may be resold any number of times.

Exchange of information among discrete government units brings into question the nature of the relationship among these units and their respective relationships to the individual. If every unit were simply an arm of an integral, amorphous, and entirely non-divisible entity, each unit would be neither separate nor discrete and, logically speaking, no information would "pass" between them. Objections to exchange then would not be supportable.

The configuration of government, however, cannot support this view of an integrated whole. Where the Income Tax Act expressly prohibits divulgence of information contained in tax returns⁽¹²⁾, it recognizes the legal independence of the Taxation Branch the Department of National Revenue. This is all but indicative of many general divisions amongst units within government.

The separate units that maintain records are distinguishable by the specific tasks with which each of them is charged. Drucker⁽¹³⁾ has stated that confining each institution

to its specific task and mission is the one dependable safeguard of freedom in a pluralist society. Insofar as each of the various units may reflect the plurality within our society, his reference to regulatory agencies in this regard may be applicable to all government units which discharge a regulatory function.

In a large measure, any exchange of information that does occur in government does so on an ad hoc basis. Few, if any, units are subject to legal requirements or policy directives obliging them to pass particular information they may collect on to another unit. It is likely though that a unit will communicate knowledge of fraud or breaches of the peace to an enforcement agency unless this is legally prohibited⁽¹⁴⁾. Leaving these exceptions aside, information exchange is informal rather than procedural, and probably, carried on almost exclusively by senior personnel. There may well exist internal policy directing clerical and support personnel not to divulge information if asked, but to refer the matter to a supervisor. Exchange commonly may take place at this level, even if not on a regular basis⁽¹⁵⁾. The individual is thereby left without any power to control the extent to which his identity is communicated within government.

The prime privacy danger lies in the environment of bureaucratic discretion - arbitrary power in the hands of functionaries who are neither politically nor legally responsible

to data subjects. While both discretionary and automatic exchange of information will violate individual privacy, discretionary exchange is the more dangerous as it is clandestine. The individual thus can never be secure in his relationship with a particular unit of government, and is not presented with the choice of communicating or withholding information that may ultimately prejudice him. The object of the entire exercise in search of privacy protection is to subject the exchange of information to rules and to give it visibility⁽¹⁶⁾. The individual must still be left with the choice to communicate or withdraw.

3. Privacy Safeguards

Comprehensive privacy controls require the establishment of privacy-oriented "rights" for subject individuals together with an instrument by which the privacy obligations of those who operate systems may be enforced. It should be noted here that use of the word "right" is restricted to its colloquial sense to mean ability or power resident in the subject individual, and carries with it a coincident duty on the part of the responsible system personnel. It does not carry with it judicial supervision but rather is used in an administrative sense, and therefore implies a regulatory structure within which these rights may be enforced.

A concurrent set of procedural or administrative safeguards is required in addition to the formulation and

establishment of the above-mentioned rights. Beyond these collateral obligations which arise are a series of non-contingent obligations which must also be assumed or imposed. In their totality, they represent a two-dimensional scheme which, when married to an enforcement apparatus embodied in a regulatory instrument, will provide the administrative protections that the environment demands.

3.1 Administrative Safeguards

3.1.1 The Nature of Regulation

Although imposed by law, the fundamental nature of regulation is political rather than legal. The normal instrument of regulation is the regulatory or administrative tribunal, a creature of the executive notwithstanding its "independent" appellation. Established to remove partisan influences in decision-making relating to the individuals and enterprises within their sphere, regulatory agencies nevertheless remain essentially political. Although the procedure of regulatory agencies may have the aura of the judicial, their members remain free to bring to bear upon the decision-making process their own personal experiences and knowledge. They usually are not subject to superintendence by ordinary courts, are subject to appeal only on matters of strict law or denial of natural justice, and are charged with executing policy. Their competence to administer policy on behalf of the political authority is the very reason

for their existence. In so doing, they operate in "public interest", as defined by the current political structures.

Under the interrogatory title of Regulation: Instrument of the People or Tool of the Interests? Krislov and Musolf state:

"Political power, when exercised, is never neutral. The reason for its exercise is indeed to take sides in some sense. A political structure and the processes generated by such a structure have consequences felt in the allocation of scarce resources of a society - economic goods, status, values, and power itself."(17)

The regulatory instruments are part of these political processes, in the sense of being the creatures of the structure. Up to now, they have mirrored the image of public interest engendered prevailing political forces.

In Canada and in the United States, regulation has been confined primarily to monopolies and the allocation of scarce resources. There has also been regulatory activity in society for the preservation of general safety and welfare, as in the case of drug and hazardous products legislation. These areas, principally the monopoly context, have come to be regarded as the norms against which the effectiveness of a regulatory mechanism of control has been evaluated.

The history of regulation, particularly in the United States, has been less than ideal. Roger Noll states that failures

result from a blend of accident and will:

"Regulatory failures are largely the result of inadequate information and cumbersome decision-making procedures, characterized as error by incompetence, or are due to the fact that regulators pursue objectives that are not in the public interest; their mistakes are errors by design." (18)

The historical circumstances which created the need for regulation are foreign to the data bank issue. Since the fundamental value of privacy of individuals is one of the interests involved, the classical formulation of public interest under which most regulatory decisions have been taken is not valid for the data bank environment. The competing interest to privacy is a diffuse value. There is no adversary situation of competing private interests, as is the case in monopoly regulation. An imbalance between social and individual needs requires regulation where the political process alone will not offer sufficient expression of individual interest. Regulation may ensure that information practices that offend against individual privacy serve social interests, that the social interests served are legitimate, and that, in all cases, a proper balance (demanded by our constitutional history) be maintained. The latter demand is quite straightforward - our laws and procedures should recognize that an individual must have the ability to determine the extent to which information about him will circulate.

Where this ability is restricted, it may only be because of an overriding social need. When government's need in this context does not reflect a need of the society at large, its whim should not provide the excuse by which individual interest can be breached.

Legislative intervention in problem solving can take either of two essentially different forms. The statute may create clear rights, or may simply establish a mode of control over rights or benefits resident in citizens. Data bank regulation is primarily concerned with this second statutory approach. In a majority of cases in other jurisdictions where statutory controls have been formulated, an administrative mechanism has been created, both to articulate privacy protective standards for data bank operations, and to receive complaints for violations of these rules. The control initiated by statutory intervention has been administrative.

There have, on the other hand, been instances where statutory intervention has set up a system of judicial rather than administrative control. Civil rights legislation in the United States, for example, has created a series of individual rights by statute which, when infringed, can be enforced in the ordinary courts. Data bank regulation, however, does not appear to allow for statutory enactment of rights in the individual which will be enforceable before the courts. Privacy itself

is not the subject of legislation; it is only the object or the goal. Regulation addresses itself to the operation of the data bank for the sake of placing a limit on those information-keeping practices which intrude into the privacy of individuals. It creates nothing more than a framework for the legal nature of privacy itself. The framework - the perimeter of acceptable information practices which regulation will fashion, must consider competing needs on both sides.

Krislov and Musolf⁽¹⁹⁾ state that, "the basic criticism of the regulatory process and administration has hinged upon two major points." They argue that government regulation is essentially a "violation of the principles of economics, necessarily less efficient than the free market place and, therefore, to be avoided." Their second criticism relates to the fact that, "administration generally violates the principles of the 'rule of law' and therefore leads to tyranny."

"Regulation" of government data banks by government itself produces a series of reasons for distinguishing it from regulation in the more common context of public utilities. Government data bank regulation is internal, exclusive to the government itself. It does not affect the public in the corporate sense, is not designed to replace market control, and is not

related to policy objectives formulated in the light of economic goals. Competing interests within the public are not in issue here; regulation will affect only the individual. Since internal administrative control, as in the case of Treasury Board authority for example, is normally exercised out of public view, the individual file subject must be given access to the regulatory structure. Although subject to rules and guidelines, self-regulatory models are generally deficient in that their processes are not sufficiently visible for the government data bank environment.

Government data bank controls will provide individual file subjects with rights enforceable against data banks upon satisfaction of a privacy violation. When regulation has been set up in the past, access to the courts against or in lieu of regulatory proceedings has been impeded by carefully drafted privative clauses. Appeals against decisions have been limited to matters of law or jurisdiction, and judicial supervision of regulatory proceedings has been restricted largely to matters of jurisdiction and violations of natural justice. Policy guidelines have, in some cases, allowed for a case-by-case resolution of conflicts and have produced a patchwork of criteria for regulatory determination of issues. The individual was not considered relevant to regulatory processes, usually never appeared at hearings, and may have been adversely affected without any real

ability to object. A regulatory structure which entertains individual presentation or representation is largely unknown. The individual interest in the data bank question is similar to consumerism and consumer representation in economic regulation. In both instances the individual has to confront the regulatory process which ultimately affects him, and must be given greater opportunity than classical regulatory forms have allowed. Inflexible rules and procedures which tend to block representation of individual interest will need readjustment.

Another legislative choice is to interpose an ombudsman or client-advocate to represent individual interest to the regulatory structure. An ombudsman can carry individual complaints to the administrative structure with which he is familiar and, generally, can succeed in satisfying a complaint by reason of the influence of his office, even if he does lack real power. The individual might then have a form of access to the administrative apparatus that would supervise data bank operations, one which would produce results and allow the individual to keep himself clear of the bureaucracy and inflexibility that characterizes administration and regulation.

Statutory intervention by government will not solve all privacy problems. The limits to a privacy claim in all

circumstances cannot be set out in legislation. An administrative tribunal charged with the duty and power to protect individual privacy against intrusion by means of record-keeping practices must become a court of record where its decision may influence or shape the criteria for privacy resolution at large. It will only address privacy incidentally by focusing on data banks themselves. It will only become a credible privacy protective mechanism to the extent that it can become cognizant of individual interest and reflect a disposition favourable to privacy in its policy. Internal administrative regulation normally satisfies its own needs and may not prove successful in the context of information systems. Strict guidelines may be required to give adequately the individual reason to believe that his privacy is sufficiently secured and, where necessary, the means to enforce his rights that regulation itself is designed to protect.

3.1.2 Licensing or Registration

Both methods have been advocated in various legislative bills introduced to control data banks and protect privacy. The Control of Personal Information Bill (U.K. 1971, Huckfield) required anyone "who is responsible for the operation, maintenance, or use of any store of information containing details of individuals" ...to obtain a licence from the Data Bank Tribunal it set up, s. 6(1), amongst which was included in those operated by the Crown, s. 16(2). On the other hand, the earlier Data Surveillance Bill (U.K. 1969, Baker) only required registration

of similar systems. The 1969 Bill did not call for an inspection procedure to ensure that systems complied with the obligation to register. The 1971 Bill corrected this oversight by proposing the establishment of the Data Bank Tribunal that would both issue the required licences and ensure compliance with any conditions appended thereto.

The major difference between licensing and registration lies in the nature of the requirements each place upon the subject. A requirement to obtain a licence implies a legal inability to operate without one. It permits individual regulation by way of conditions incident to continued holding of a licence. Registration requires a subject to inform the state of the fact that he is carrying on a particular operation. The obligation to register does not carry with it discretionary power by the state with respect to controlling entry into the field. Regulatory control, if exercised at all in these circumstances, is effected by means of rule-making in terms of the whole field or its specified sub-areas. As a vehicle for preventative regulation, licensing is generally considered to be more effective.

3.1.3 Authorization for Information Exchange

A total ban on information dissemination and exchange would be the most direct means of ensuring that such practices do not continue to be clandestine and unregulated (government data

banks only excepted). Another possibility, one less direct, may be to formulate sets of circumstances and conditions wherein communication of files will be allowed. A specific petition to the regulatory structure would not be necessary, the only state function necessary would be the policing of the system to control abuses. In the licensing model, the above conditions could be set out in the terms of various licences. Under a simple registration scheme, the criteria for dissemination could be promulgated from time to time for different classes of systems, (difficulties may arise, though, due to different conditions in particular cases). In both systems, the subject would be notified of the divulgence. When applied to situations of regular and constant communication, these procedures would subject routine communication to an articulated set of conditions, make it visible, and streamline its regulation. When circumstances dictate a need for supervision of exchange, this procedure will provide a mechanism by which this can be implemented.

The inherent weakness of this approach results from the nature of the information dissemination and exchange that is actually carried on in an operative system. No particular system lives off another on a regular basis as the source of its data. An ad hoc procedure is required for exceptional cases where the demand for dissemination or exchange is tied to a need

to know, the legitimacy of which may be the subject of inquiry. Since conflicting interests arise in this circumstance, the proper resolution of the conflict requires their expression and consideration. An adversary rather than an inquisitorial procedure allows for expression of the conflicting interests and necessarily enhances the importance to be accorded to the subject of privacy itself. Where divulgence is permitted by decision of the regulatory instrument, the need to know will have been balanced against the validity of the contrary privacy claim.

The adversary procedure is ad hoc only in the sense of being initiated whenever the need arises. Resolutions of conflicts occur subject to criteria which the tribunal itself can promulgate. This approach, unlike the first, allows for flexibility; it will permit the resolution of conflicts tailored to the specific circumstances of each case. In short, it recognizes the role of the tribunal as an arbiter with respect to the competing parties, rather than as an advocate of either.

Authorization for divulgence of particular information, when necessary, can be made subject to a rigid procedure. The requesting party might be obliged to obtain a warrant, or writ, from the regulatory tribunal upon presentation of a prima facie

case of legitimate need and public interest. The issuance of the writ could carry with it notice of a hearing on the merits of the claims advanced by data bank and the subject, plus an invitation to the respondent to contest the application. Once final approval is given, the individual could be allowed a delay to gain access to his record for verification purposes before the authorization itself is executed. Insofar as this exchange may ultimately affect the individual adversely, this procedure would ensure that some of the more basic rules of natural justice are observed.

3.1.4 Exceptions

It is likely that several exceptions to the above procedure will be necessary. Where information is held under an arrangement of confidence, as are tax returns, the same procedure would not be available. Authorization legitimately could not prevail against existing statutory guarantees. In addition, the above procedure might not be necessary where dissemination is only a vehicle for policing the system itself⁽²⁰⁾. Investigations of welfare fraud, for example, would require information stored by National Health and Welfare to be made available to law enforcement agencies. In this case, the law enforcement agency should not have to seek authority to obtain the pertinent data, as it may be assumed that National Health

and Welfare has both the right and the duty to supervise the schemes they offer.

A further exception may be necessary in reference to law enforcement agencies generally. If the circumstance should arise where information held by one unit is required for the sake of evidence in a criminal proceeding, the above-described authorization procedure would not appear advisable. The information sought might be dealt with under the laws of evidence, and released pursuant to a search warrant obtained in the usual fashion under the Criminal Code. A further condition might be imposed by making this information available only when it refers directly to a prosecution of the file subject himself, and where the information was not obtained from him under legal obligation in the first place. The existing confidentiality provisions would continue to apply.

The role of the tribunal in the context of authorization for dissemination of data will not be strictly and exclusively judicial. In its administrative capacity, the tribunal is specifically charged with the duty of acting in the name of the public interest, which includes the individual's interest in his own privacy. In any authorization conflict, the tribunal should not be bound by strict judicial practices, as regards both procedure and evidence. It must recognize the general ability of individuals to present their own case for non-disclosure and

privacy. In every case, authorization should issue only after the tribunal is satisfied that disclosure of information is necessary rather than simply useful, that it serves more than the plain need of efficiency, that (where possible) it will not react adversely on the individual, and that the released information will not be passed on to another party. The tribunal must not be made subject to pressure of any kind and must, above all, realize that authorization to release information - to allow, in effect, a violation of a trust relationship between citizen and government - must remain exceptional. Its own role will be rendered meaningless if authorization becomes commonplace.

3.1.5 Other Administrative Obligations

There is a variety of obligations which might be imposed upon data banks that will afford greater privacy protection than at present. These duties would provide information about the systems to the regulatory tribunal, which will thus become knowledgeable of the extent, nature, and use of information contained in these systems. A determination of the risks to privacy posed by them may thus be intelligently made in each case. Every administrative data bank might properly be required to file a profile describing the extent of its records, its sources of information, its technical and physical security arrangements, the authority under which the records are kept, and the officers responsible for the system itself. The profile

could also explain the purpose of the system. Once armed with these facts and figures, the tribunal would be in a position to determine when release of data is necessary, and whether particular systems adequately protect their data. It would also be able to decide whether the information stored by any system exclusively serves the purposes of that system. Furthermore, it could evaluate the level of redundancy of stored information with government generally. These obligations are all workable under either a scheme of licensing or simple registration.

3.2 Rights of the File Subject

Much has been written about the risks to privacy and the consequent need for access and verification control by the subject. Richard I. Miller⁽²¹⁾ states that legal requirements for data bank operators should include giving subject individuals access for the purposes of verification. The Data Surveillance Bill (U.K.), 1969⁽²²⁾ would allow any person to apply to the Registrar (proposed by the Bill) for an order that any or all of the data contained in a particular data bank be amended or expunged because it is incorrect, unfair, or out of date in light of the purposes for which it was stored in the data bank. The Bill, and the writers who have argued for verification, has produced an enlargement of the issue which should be considered.

The argument of privacy has been used to call for regulation of data banks. Writers have argued for protection in such regulation for rights not strictly limited to privacy alone. Karst(23) sees the question of data accuracy to be relevant because of reasonable fears that may be held by the file subjects. He claims that we "worry about widespread access by third parties because we doubt the accuracy of the information passed along from one file to another, and we worry about accuracy partly because we fear that efforts to limit access will fail." In this sense, he sees access and accuracy to be complementary. Since third-party access does relate directly to privacy, its pertinence to accuracy would make the subject of accuracy itself relevant, even if not consequential.

Accuracy should not be a true test of intrusion. Disclosure to a third party is the act by which individual privacy is breached. The implication here is that derogatory information might be considered private to the subject, while non-derogatory information might not. The argument would then be that communication of false information of a derogatory nature invades privacy, and is necessarily as harmful as derogatory information which is accurate. Verification control would strike at the issue of privacy only where the inaccuracy is derogatory, and consequently the right to verification on behalf of privacy is more closely tied to the derogatory character of the data rather than to its inaccuracy.

Although not directly related to privacy protection as such, the question of access for the sake of verification should be examined. The regulatory circumstances for privacy protection are suited to protection of other rights that may also be threatened by information processing. When information is the basis for determining eligibility for welfare, for example, false information might well threaten it. Verification would become a necessary means by which the benefit may be sustained. What is at stake here is not so much the privacy of the individual as his right to be treated fairly, to participate on an equal basis in public and commercial relationships, and to be evaluated in terms of standards applicable to all.

Decision-making on the basis of false, inaccurate, incomplete, out-of-date, misleading, or biased information threatens this right and interferes with the fair and reasonable application of these "civil rights". The accuracy of data relates to the decision-making process and to the potentially harmful consequential effect on the subject; it should properly be within the supervisory competence of the regulatory tribunal. Access could be granted immediately upon creation of the file and at regular intervals. Since the great majority of these files are maintained in Ottawa, access might be effected by means of supplying the subject with a print-out instead of requiring

that he present himself in person at the location of the system itself⁽²⁴⁾. Finally, where an individual becomes aware of an inaccuracy, a procedure for challenge must be set up to make the right of access meaningful; in this situation, he might petition the tribunal to order correction or deletion as circumstances require.

Administrative rights in the hands of individual subjects of government operative record systems may be summarized as follows:

- i) Access - the individual has the right to know what information about him has been collected and stored. This could be extended to give the subject the right to know what is being collected.
- ii) Correction - The subject may challenge their accuracy and timeliness of entries. A standard for obsolescence⁽²⁵⁾ could be established by the regulatory body with respect to particular kinds of data stored in the various systems. Challenge may be made to the regulatory body which may determine upon whom the burden of proving the accuracy of the data lies.
- iii) Notification - The subject should be notified of changes in the record and, where authorized, release of data. He might even be informed of intention to seek release if a warrant or writ procedure for authorization is adopted. For changes in the record, he could be supplied with a print-out at regular intervals.
- iv) Compensation - The subject might be awarded compensation by the regulatory body for damages suffered due to infraction of statutory rules and regulations that protect his rights. Compensation might be awarded for specific loss upon proof, or a minimum sum might become payable in response to a violation even if no loss can be proven

The value of these rights for file subjects lies not only in the specific remedies made available in defence of personal privacy, but also in the general effects of the corresponding obligations. Sanctions created against privacy violations arising from misuse or disregard of rules will raise the level of sensitivity to the entire privacy issue itself, and specifically to the damage that unsecured or misused records may cause. Record systems personnel would be educated in the degree to which they are personally charged with not only a public trust but, more significantly, with a duty of care to each individual identified in the records, since their neglect will affect the particular individual himself.

d) Collateral Safeguards

1. Technical & Physical Arrangements -
"guarding stored information"

Technical and physical arrangements are necessary to complement the above-described administrative procedures⁽²⁶⁾. Such procedures alone cannot render stored data secure from unauthorized and clandestine penetration, since they counteract only those privacy risks that arise from conventional record-keeping and data exchange practices. Technical and physical means provide security against risks that do not fall within those normal data operations executed on a day-to-day basis.

The level of security built into any system should be selected with due regard to the threats to privacy inherent

in the system. Since all information systems containing individual records are deemed to threaten the same loss of the individual's privacy when penetrated, all require security arrangements. Distinctions in how much security is necessary in each case are mandated by extrinsic, non-privacy related, factors. Police systems, for example, may require greater built-in protections because there may be greater inducements for the subjects of such systems to attempt to penetrate them. Additional protective measures stand to be required by police systems, though it is to be noted that this is a consequence of factors present in such systems which are entirely unrelated to the extent to which they stand to lessen personal privacy in the event that the system's integrity is compromised.

Once hardware and software devices start to make the cost of intrusion higher than the benefits to be derived from successful penetration, the actual level of security that should be attained is quite a moot point. Since cost considerations for security are involved, a security standard for subject systems is required. Sub-groups within administrative systems can be set up for these purposes. Where, for example, a system has remote terminal input/output access, terminal and user identification will be a requirement. Whether, in this case, user identification will be implemented by means of a password or a complicated algorithmic routine will depend on just how much

money is available. Similarly, encoding for both storage and computer-terminal communication will be governed largely by costs. It is unlikely that one standard can be made to fit all cases, given some legitimate differences in security needs and discrepancies in funding amongst the various departments and agencies.

Physical arrangements, such as limited personnel access to record centres, proper identification techniques, and surveillance, will complement the technological methods of protection that may be built into the systems themselves. The standard of physical security too will be based upon relative need and acceptable costs, and will vary from one system to another.

2. Personnel Security - Clearance and Bonding

A supplementary privacy safeguard will be incidentally provided by the staff of record-keeping units. A staff educated and sensitive to privacy and the risks posed by systems and practices, may, in the long run, prove to be one of the most effective safeguards.

Normal security practices call for clearance of staff in risk positions. Ironically, security clearance is itself essentially privacy intrusive. The forms required for civil

servants, for example, which call for family information, personal scholastic and employment histories, and references can create quite a comprehensive profile of the applicant. At the same time, clearance is deemed to be necessary for the avoidance of unnecessary risks that may be posed by vulnerable candidates, whether socially objectionable characteristics are relevant to the candidate's ability to perform his job tasks or not. The need for clearance is observable for airline pilots, for example, to assure that an applicant with an unfavourable medical history will not be engaged. Similarly, a bank will not engage personnel with criminal histories, particularly those who may have committed theft or fraud. In other cases, the need for clearance is less obvious and perhaps even doubtful, particularly where something in a personal history has nothing to do with eligibility criteria for a job. In all cases, there is a trade-off between the privacy of the employee and the need for information determined by the employer. The question of security clearance is largely academic in relation to government systems. The personnel all will have been examined in the normal procedure for civil servants generally.

A further requirement of bonding may be considered in this context. Bonding is normally used as a supplementary measure of indemnification against civil liability. Banks require bonding so that in the event of fraud by a teller, for example, where

the bank is vicariously responsible for loss to a client under a master-servant relationship, it can recover the loss from the insurance company providing the bond.

This procedure could be applied to information processing in government. Greater attention to considerations of personal privacy might well follow from some scheme creating civil liability in the Crown for violations of the privacy of the subject. Such liability should motivate a reappraisal of methods and procedures and would necessitate greater regard for the quality of staff. If bonding were required, a central clearance authority for bonded personnel could be established so that eligibility requirements would be uniform. One model for such an arrangement might be a professional association which would not only certify personnel as to competence, but would also guarantee fidelity by means of a fund set up to deal with claims against members occasioned by their incompetent or fraudulent behaviour. Such a system is found frequently in the legal profession; examples exist in funds established by the Quebec Board of Notaries and by the Law Society of Upper Canada.

Since the procedures that come with bonding, such as personnel investigations, are privacy intrusive themselves,

bonding should be required only after a clear appraisal of what it may accomplish in a given context. If personal privacy is to be traded off for a theoretical protection of doubtful value, so that the privacy of the few is compromised and the privacy of the many not significantly enhanced, bonding should not be required. The privacy of the few is also the proper concern of this Task Force.

3. Self-Regulation - a Professional Society

Self-regulation is not intended here to relate to the regulation of government's own data banks by government itself. It relates to the establishment of a regulatory body drawn from the data processing environment itself, and is not specifically limited to government personnel alone. Law societies and colleges of physicians are models of self-regulation. One might ponder whether these models are applicable to the data processing environment, whether such a structure might protect individuals from abuses of their rights.

Self-regulation entails the establishment of a virtual guild system for information processing personnel. Members of the structure stand to have their conduct supervised and evaluated by their peers, yet on the other hand, the structure will also serve to protect the interests of members from outside challenges.

Self-regulation, as in the case of doctors and lawyers, is an example of delegated administrative power. By means of statute or charter, medical associations and law societies exercise regulatory functions which would otherwise remain with the state. These societies establish codes of suitable conduct, set criteria for entrance into the profession, and certify competence. In many instances they are competent to deal with complaints and settle conflicts.

These societies literally replace, under public authority, the state in its daily routine of regulating such professions in the name of public interest. Like most regulatory bodies, these professional societies are protected from judicial supervision by the usual privative clauses which serve to frustrate appeal to courts of law in most cases. Furthermore, they are more independent of political control than are state regulatory agencies, and are more closely aligned to a distinguishable corporate interest, that of their membership. Often, they work on the premise that conflict between their own interest and public interest is largely hypothetical.

At another level, self-regulation may be provided by means of a voluntary association. Unlike mandatory associations, such as the law societies, these groups are not vested with exclusive certification powers, cannot restrict entry into the profession or

trade itself, cannot punish misconduct (except by expulsion and its moral rather than legal repercussions) and are not vested with state regulatory powers. They capitalize on industry recognition of their ability to mobilize interest, their own good name, and the confidence of the public at large. Thus the British Press Council can give the public valid reason to believe in a responsible press. Similarly, the British Computer Society will assure prospective employers that its members are competent and that they will behave in a suitable manner. To the extent that the public itself may be affected, it may feel that its own interests will be similarly protected.

Voluntary associations within the data processing industry may be found in Canada. The largest of these is the Canadian Information Processing Society (CIPS), which is nationally based. CIPS formed a committee to study the question of professionalization and self-regulation for reasons which include privacy protection for individuals. The Data Processing Management Association (DPMA) is another national group with regional associations, and together with the Canadian Operations Research Society (CORS), these three groups include most individuals engaged in data processing at all levels. If professionalization is to come within the next few years, it is likely that these various groups and associations will nationalize into one umbrella organization with separate provincial affiliations. In many cases at present membership in two or even three of these societies tends to overlap.

Self-regulation by means of certification of training and competence, codes of conduct, and sanctions may not be the answer to the privacy problem posed by data banks, particularly in the government context. The delegation of power to a self-governing body is predicated on a number of important assumptions about the nature of a profession and the service it provides⁽²⁷⁾. These assumptions, in turn, may produce deleterious side effects.

Where, for example, it had historically been assumed that membership in a professional association had to be restricted to those who had the mental ability and proper temperament to absorb and use the knowledge requisite to the practice of the profession, the ensuing restriction served as a means to command higher prices. The apprenticeship requirement in the mediaeval guilds, while designed to train recruits, became a device by which professionals could make use of cheap labour over an extended period of time - in some cases up to seven years. Furthermore, there has never been any guarantee that a self-regulating society would not transform itself into an interest group and seek protection of its own interests at the expense of its duty to protect the public interest. In addition, self-regulating societies have tended to become insular, tradition-minded, and, in many instances, not responsive at all to changes that take place within society.

Legislation introduced in the Quebec National Assembly over the last year, which would limit the delegation of regulatory powers to self-governing societies and give certain powers back to the government, would tend to show that self-regulation is not working as well as it was once thought. Furthermore, the propensity toward establishmentarianism and elitism within professional groups and the resulting bureaucratization hamper effectiveness here, as in any regulatory setting.

Whether self-regulation is necessary or merely useful, whether it is effective as a means of control or simply serves as a self-fulfilling device, indeed, whether the field itself is amenable to professionalization are all questions incidental to the regulation of government systems. Their relevance would be found in the role of a professional society, which would include government personnel, in providing collateral safeguards to privacy at the personnel level. If privacy can be compromised by incompetent or negligent staff, a professional society's role in certification of membership competence, education, and training may be of importance to privacy.

If additional security clearance were required, a professional association might have a role to play there as well. The major usefulness of a professional association lies in relieving government itself of the responsibility of certifying competence based on training, as in the case of government lawyers

or doctors who are certified by their provincial professional associations. Questions as to the form that such an association may take, the powers and functions of such an association - indeed, whether or not data processing is a profession - are relevant to privacy where data banks in the private sector are involved, since self-regulation of the entire industry is in question. Professionalism, in the particular context of government systems' personnel is, therefore, of only marginal interest.

Chapter Three

The Regulatory Body

a) Requirements

Computerization, records, and information exchange in government are not matters tied directly to basic policy choices and first-level national goals. The records and systems serve government only as tools. Where controls for the sake of privacy are necessary, countervailing forces present include cost and reduced efficiency of government itself. The measurement of private interests against the "public interest" will not be dependent upon acquired rights of individuals other than the right to privacy in the colloquial sense. Since regulation here is not equivalent to those conditions of regulation at play in the private sector, the highly stylized forms that characterize the latter may not be necessary. Involved here is government regulation of itself.

If a regulatory body independent of the decision-making centres within government is required, it could well take on some of the forms and styles of the commissions and boards set up to regulate sectors in the economy at large. Similarities as to form, composition, methods and procedures will be consequences of those similarities of function that may exist. The relevant characteristic of the regulatory body lie in its relative independence,

as in the case of regulatory models generally. In this context, government may be placed in the position of the user in the normal regulatory context. The consequent independence of the regulatory mechanism proceeds from the necessary view that, in this situation, government systems cannot, with few exceptions, validly be charged with regulating themselves in their own interest (nemo iudex in sua causa)⁽²⁸⁾.

b) The Treasury Board as a Model

The regulatory role that is demanded within the context of government systems is, in some degree, equivalent to the role of the Treasury Board insofar as this body functions as the Cabinet's "Committee on Management". Data bank regulation only looks to how subject systems will remain within given modes of operation, as with the processes governed by the Treasury Board. These desirable modes would be framed in terms of the aforementioned rules for safeguarding privacy in government systems.

Notwithstanding these similarities of function, it is unlikely that such a scheme for privacy regulation would be workable. The Treasury Board lacks visibility. It has no connection to the public, is not subject to an adversarial procedure, and has no impact at all on the rights or privileges of private individuals. Its financial regulatory abilities are general rather than specific to data bank regulation. In short, the

chief undesirable characteristic of the Treasury Board as the regulatory instrument in the data bank context is its bureaucratized nature⁽²⁹⁾, it is not the compact, independent, and expert instrument that is required.

At this stage only government systems are seen as being subject to regulation. If data banks generally are to be regulated, it is necessary to create a regulatory structure that would allow for involvement outside of government systems. Even if the discussion is confined to government systems alone, however, the shape of the regulatory body could be such as to allow for extension to non-government systems in the future. Establishing the Treasury Board as the body would rule this out.

c) Alternative Approaches to Regulation

The regulatory issue, in terms of government systems alone, is unique. On the one hand, the type of control demanded is managerial and administrative; policy formulation and enforcement requirements within government itself make the regulatory function similar to that already exercised by the Treasury Board. On the other hand, visibility of the regulatory system to the public is required. The judicial requirement makes a strictly internal administrative control model unworkable. It cannot meet the basic need of subject individuals that the privacy conflict engenders - access to the structure itself.

Two possible alternatives which would provide control as well as access are available. The model of a tribunal, similar in nature and function to the Data Bank Tribunal proposed in the Control of Personal Information Bill (supra) would fit within the government context. In its administrative capacity it would establish policies that the privacy requirements demand, and impose them in the form of regulations or conditions of licence as the supervisory scheme would allow. Its judicial nature, (since it would be composed as a tribunal) would permit access to it by persons with complaints to be adjudicated.

Authorization procedure could be fashioned through a public quasi-litigious hearing - a further advantage of the "commission" format.

Another possibility lies in the form of control envisaged in the Data Protection Act (Oct. 7, 1970), of the State of Hessen, Federal Republic of Germany. Instead of establishing a tribunal, privacy control over automated record-keeping practices and systems is vested in a Data Protection Commissioner. This official is independent of Parliamentary direction (s.8) but is not totally responsible for enforcing statutory provisions regarding confidentiality of information contained in subject systems. Section 10,(1) of the Act empowers the Commissioner to "inform the responsible control authorities of any infringements committed;" it also states that he, "shall

initiate measures for improving data protection." Section 11 gives anyone who considers that his rights to confidentiality have been breached the right to apply to the commissioner. Finally, he acts in an ombudsman-like capacity in submitting annual reports to Parliament.

If either Parliament or the Cabinet were to assume the control function in the administrative sense, the Hessen model of a commissioner could be implemented. Treasury Board's present administrative powers might be employed in this field and the commissioner might become its investigative and judicial arm, thereby giving Treasury Board the visibility and accessibility it otherwise lacks. Reports could be submitted to it annually, which in turn could be tabled in the Commons by the President of the Treasury Board. The ultimate responsibility would lie in the Cabinet. Alternatively, the commissioner might be given independent status with power to call upon Treasury Board for information in any investigation he would undertake. The office of commissioner here would be similar to that of the Official Languages Commissioner. The Tribunal approach is the more favourable choice where regulation is to be extended beyond government systems along. If Crown Corporations and other data repositories with federal regulatory competence are to be brought within the ambit of enabling legislation, the tribunal model is necessary.

In this event it could be set up along lines similar to some existing tribunals, such as the Canadian Transport Commission. The composition would take into account the need for data processing and managerial expertise as well as legal input. Since the regulatory connection is to individuals directly, the responsible minister might be the Minister of Consumer and Corporate Affairs. Alternatively, responsibility might be vested in the Minister of Communications, insofar as remote data processing generally is of interest to that department.

d) Interim Measures

If regulation itself is not deemed advisable at this particular time, an interim solution to the problems for privacy created by government systems can be fashioned. The setting up of an advisory board or bureau to investigate the activity and draw attention to privacy risks could prove very useful in arresting further developments which, if unchecked, may produce an extreme situation where privacy is no longer available. The board could note privacy intrusive practices, the adequacy of existing technical safeguards, the deficiencies in basic legal protections, as well as other considerations that affect privacy. It could recommend necessary changes. Its chief utility would lie in exposing the risks to public view, so that the desirable political action might follow. At the same time its investigations

and reports could raise the privacy consciousness of systems personnel. While an advisory board could not be granted policing and enforcement duties, its recommendations could be channelled to another authority which would be competent to deal with the issues in a regulatory mode. This latter body could be an internal administrative unit.

Conclusion

As little as ten or twelve years ago, technical innovation and implementation which promised material benefits for society met with minimal resistance. The argument at that time was not with technology but with economics. Opposition was limited to those who felt that technical implementation in a specific instance would injure their pecuniary interests. Western free enterprise states were "growth" oriented. No one seriously challenged the industrial dogma of continuous economic expansion to bring material well-being for all. These societies regarded growth not only as necessary but as virtuous.

Ten years later these same societies are challenging this doctrine. Canadian society is an extreme case. We are only now beginning to feel that the price of technological development is too costly, for fouled rivers and strip-mined mountains are not the only consequences of growth. Foreign ownership, a sensitive political question, is also a product of the flirtation with all-out development. The increasing resistance to it, as in the cases of environmentally based challenges to growth, is so related as well. Fears of loss of nationhood, overcrowded and deteriorating cities, infringement of nature, contamination of our food and water supplies - cries which formerly were unheeded are now the concerns of governments. So too is privacy consciousness, which has been aroused largely

in reaction to technical development. It is only since it has become legitimate to question the virtue of technology and growth in general that privacy consciousness has begun to assert itself.

If privacy has ecological overtones to it, they are more individual in this case than in strictly environmental ones. They are also political. Infringement of dignity and destruction of personality, these potential consequences of privacy deprivation, are threatening to each man as an individual. He will see society as a goldfish bowl wherein he is called upon to conform to standard patterns of conduct, perhaps not for fear of reprisal but rather for fear of attention by virtue of his being different. His own existence ceases to be unique; he is threatened with becoming nothing more than a nameless, faceless folio number identifying him in a file. Notwithstanding real needs for positive identification of individuals in many social instances, there exists a fear, not totally supportable by reason alone, that absolutely positive identification destroys the sense of personal identity. ⁽³⁰⁾ Privacy, the state of not being involved in the perceptions and deliberations of others, protects that uniqueness.

We also fear the political consequences of loss of privacy, although, ultimately, these threats reduce themselves

to the same individual effects outlined above. The power ratio is a function of the level of interaction between the individual and state. Loss of privacy upsets the balance adversely for the individual. Governments are called on to provide the means by which society may harness its disparate energies to produce social well-being. Our western constitutional traditions have tended to produce an equilibrium between the force of the state and the rights of individuals through which all well-being might be attained. The process of balancing opposing forces is continuous, the pendulum swinging from one direction to the other and back again. The destruction of individual private realms can throw the trajectory of the swing off-center. The preponderance of power may irreversibly shift to the state, leaving the individual not only with reduced power, but also with a reduced ability to alter the course of the power shift. The state can lose sight of its role as delegatee of sovereignty and exercise power in its own name. It is a delicate thing - to place the responsibility of acting against social evils upon the state by making power available to it, yet to ensure that no profit to the state is derived in its own interest. A century ago Mill articulated this dilemma:

"To determine the point at which evils, so formidable to human freedom and advancement, begin, or rather at which point they begin to predominate over the benefits attending the collective application of the force of society, under its recognized chiefs, for the removal of the obstacles which stand in the way of its well-being; to secure as

much of the advantages of centralized power and intelligence as can be had without turning into governmental channels too great a proportion of the general activity - is one of the most difficult and complicated questions in the art of government."(3f)

Information is a new power base. In the hands of government it can be a useful instrument for decision-making in aid of individual and social betterment based upon reason. The use of the tool, however, must be restricted, for it may corrupt and divert government from its primary role. Restrictions in the name of individual privacy are not merely useful but necessary to these ends.

Our common political and intellectual tradition, emphasizing as it does the primary value of personal liberty, allows for a multitude of avenues for future social development. Yet it is becoming increasingly evident that one present danger to the continued development of a free and liberal society is the tendency towards centralization of political power in the hands of those able to accumulate and manipulate vast quantities of personal information.

It is to be emphasized that no more than a tendency towards such a power realignment based upon data accumulation can be discerned at present. It is clear to all that the trend in this direction - especially in Canada, less so in the United

States, for example - is yet to reach such proportions as to have any marked effect upon the day-to-day political processes. The trend which is observed is yet in its infancy. Still, a danger - albeit an incipient one - is posed to the delicate balance between freedom of the individual and the coercive powers of the corporate state.

Because of the relative size of the federal government sector, and for this reason alone, the potential effect of information practices at this level warrants special attention. The question of information has long been recognized as one of power, and this study has centered upon those steps which can be followed to assure that extrinsic forces related to government data practices do not result in an unintended reallocation of power and liberties within our system - a reallocation irrespective of, and quite possibly counter to, the value allocations desired by the people of Canada and intended by their elected representatives.

Notes

- (1) Perhaps the best definition of a data bank is the one developed by the Manitoba Law Reform Commission:

"An information storage operation which can supply personal information about a specific individual identifiable by name or means through which the name may be readily obtained."
- (2) Oxford Group of the Society of Labour Lawyers, Report on the Right to Privacy, March, 1971, 28.
- (3) Compiled by the Manitoba Law Reform Commission (see note no. 1)
- (4) Personnel records of civil servants should not be classified as non-operative even though they are maintained for internal purposes. These records are the bases upon which decisions are made respecting transfer, promotion, dismissal, etc., all of which directly affect the subject's status and opportunities. For this reason these files are "administrative."
- (5) R.S.C., 1970, c.S-16, s.15(1)

"No individual return and no part of an individual return made, and no answer to any questions put, for the purposes of this Act, shall, without the previous consent in writing of the person or of the owner for the time being of the undertaking in relation to which the return or answer was made or given, be published, nor, except for the purposes of a prosecution under this Act, shall any person, other than a person employed by the Bureau or working under arrangement with the Bureau and sworn under section 6, be permitted to see any such individual return, part or answer."
- (6) *ibid*, s.15(2)

"No report, summary of statistics or other publication under this Act shall contain any of the particulars comprised in any individual return so arranged to enable any person to identify any particulars relating to any individual person or business."
- (7) s.91(27) B.N.A. Act, 1867.
- (8) SEARCH is the acronym for "Systems for Electronic Analysis and Retrieval of Criminal Histori-s."
- (9) Phil Hirsh, "L.E.A.A. Who Guards the Guardians," Datamation, June 15, 1971, 28.
- (10) On Record, Stanton Wheeler, editor, Russell Sage Foundation, New York, 1969, 25

- (11) Data security is the subject of a separate report to the Task Force. The reader is advised to consult that report or the General Report, c.9, p.101.
- (12) R.S.C. 1970, c.I-5, s.196(1,2,3,4)
- (13) Peter F. Drucker, The Age of Discontinuity, Harper Row, New York, 1969, 250.
- (14) A curious example, quite unlike anything in this country, is the narcotics registration system in Britain. Under the Narcotics Addiction Registration Act a central register is maintained for all those who have chosen to participate in the courageous government scheme to supply narcotics to addicts as a means of preventing drug-induced crime. The register contains the name, address, and description of the specific addiction of each registrant. It also contains the name of the administering doctor since each registrant's name is actually communicated to National Health Service doctors who administer the drug from selected hospitals and clinics, or offices. Furthermore, the names and addictions of the registrants are even given to local police so that they may know who is in legal possession of the particular narcotic. In this way, the registrant will not be harassed, and will actually be left alone. In a curious sense, his privacy will be safeguarded.
- (15) Such practices were revealed by The Guardian to be quite common in the British government (May 11, 1971). The article stated that the usual procedure followed was for the official seeking the information not to ask for it in writing but call up the official who "might know" something about the subject and receive the information over the telephone.
- (16) See "L'informatique dans l'Administration Française," p.VII - 10, Raphael Hadas-Lebel, rapporteur, presented to the Congrès de l'Institut International des Sciences Administratives, (Rome, September, 1971).
- (17) Krislov and Musolf, The Politics of Regulation, Houghton & Mifflin Co., Boston, 1964, 70.
- (18) Roger Noll, "The Causes of Regulatory Failure", Private Address.
- (19) op. cit. 18
- (20) This recommendation is taken from a confidential and unpublished working paper of the President's Commission on Federal Statistics.
- (21) Computers and the Law, edited by I.P. Bigelow, (American Bar Association Standing Committee on Law and Technology), 2nd ed. 1969.
- (22) s.5(1)
- (23) Kenneth Karst, "The Files: Legal Control over the Accuracy and Accessibility of Stored Personal Data," Law and Contemporary Problems, vol. 31 (Spring 1966), 342.

- (24) The Public Service Commission supplies printouts to 6,500 civil servants who participate in DATA STREAM, an automated personnel management system for specific categories of employees. The employee, upon receipt of the printout in duplicate, will verify it and actually make additions or corrections where required. These data are entered into the system to become part of the subject's file. This system might be considered a model for all administrative systems obliged to provide printouts to subjects.
- (25) The question of data obsolescence is a complicated one. In some instances, the regulatory authority might see fit to ensure expunging of all original data upon the expiration of a given period of time. Regard must be had, however, to statutory rules which govern particular circumstances and/or relate to evidence. An example may be found in bankruptcies. Under Rule 64 of the Bankruptcy Act records of a bankruptcy must be maintained for 14 years in case of fraud appearing after discharge. Provincial laws might also appear in this connection. For example, where individual records containing description of contract debts are ordered expunged after a delay of two years, this will conflict with provincial laws which make debts claimable for 5 or 6 years, depending on the province. The expunged record will not, in this case, accurately reveal the true financial state of affairs of the subject.
- (26) This section is not meant to be comprehensive. For full analysis of technical means of safeguarding stored data, see Task Force Report No. 5.
- (27) Report of the Commission on Post-Secondary Education in Ontario, "Certification and Post-Secondary Education," December 1971, 22.
- (28) A curious regulatory structure within government lies in the office of the Official Languages Commissioner. His powers are not delegated by the executive branch but are conferred by Act of Parliament. His independence of the executive would tend to make him less the captive of the administration which he will regulate.
- (29) It is necessary in this context to distinguish between Treasury Board and the Treasury Board Department. Treasury Board is a 6 Minister Committee of the Privy Council; the Department is the bureaucratized infrastructure responsible for performing the functions endowed upon the Board.
- (30) Instant World, A Report on Telecommunications in Canada, Ottawa 1971, 42.
- (31) John Stuart Mill, On Liberty, Crofts Classics edition, 116

REFERENCES

The Age of Discontinuity, Peter F. Drucker, Harper Row, New York, 1969.

On Liberty, John Stuart Mill, Crofts Classics Edition.

On Record, Stanton Wheeler, editor, Russell Sage Foundation, New York, 1969

The Politics of Regulation, Krislov and Musolf, Houghton and Mifflin Co., Boston, 1964.

Computers and the Law, Robert P. Bigelow, editor, (American Bar Association Standing Committee on Law and Technology), 2nd ed., 1969.

L'informatique dans l'Administration Française, Raphael HADAS-LEBEL, rapporteur, Rome 1971.

Report of the President's Commission on Federal Statistics, Washington, 1971, 2 volumes.

Certification and Post-Secondary Education, Report of the Commission on Post-Secondary Education in Ontario, December, 1971.

The Right to Privacy, Report of Oxford Group of Society of Labour Lawyers, March 1971.

Instant World, A Report on Telecommunications in Canada, Ottawa, 1971.

Datamation, June 15, 1971.

Law and Contemporary Problems, vol. 31, (Spring 1966)

INDUSTRY CANADA/INDUSTRIE CANADA



61137