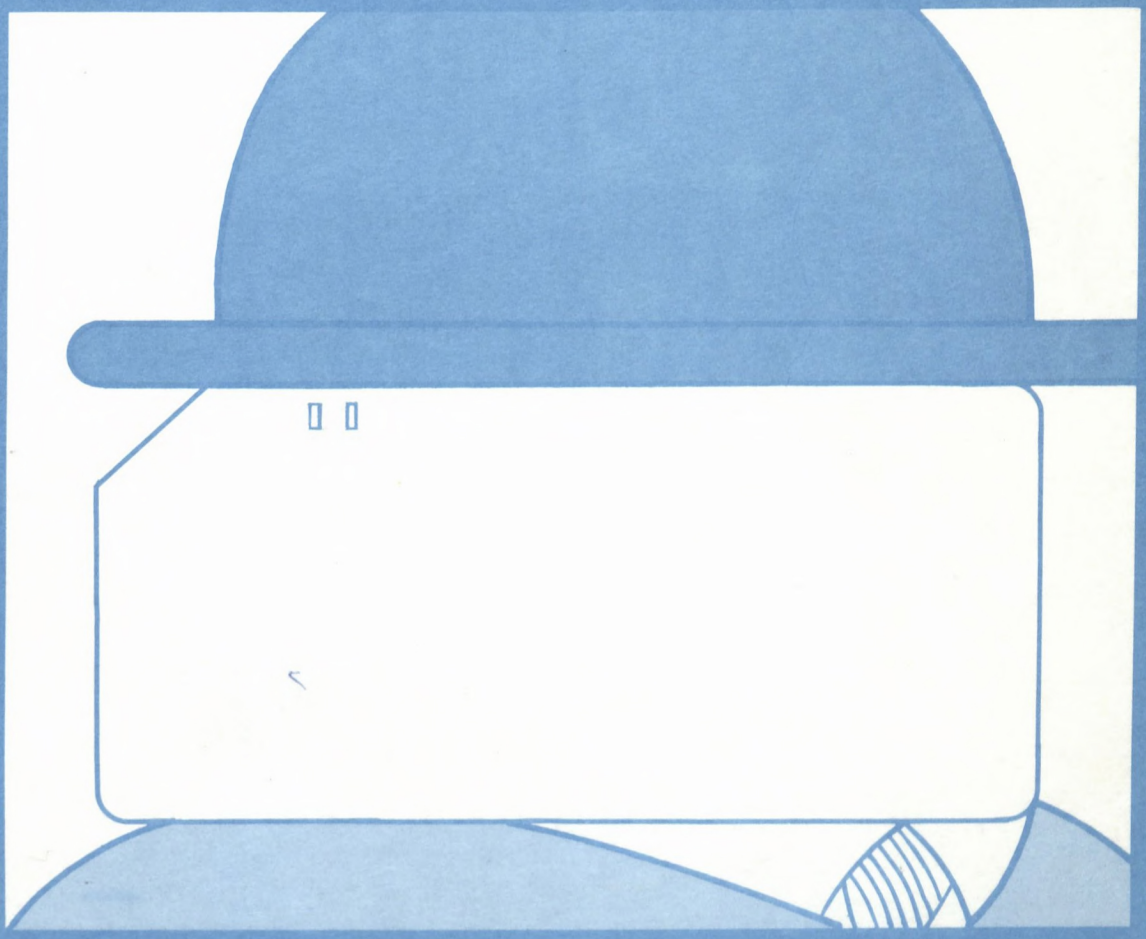
REGULATORY MODELS

J.M. SHARP



2. A study by the Privacy and Computer Task Force

REGULATORY MODELS

A STUDY FOR THE

PRIVACY AND COMPUTERS TASK FORCE

DEPARTMENT OF COMMUNICATIONS

DEPARTMENT OF JUSTICE

J.M. Sharp

This report was prepared for the Privacy and Computers Task Force, an inquiry sponsored by the Departments of Communications and Justice, and should not be construed as representing the views of any department or of the Federal Government. The views expressed herein are exclusively those of the authors, and no inference of any commitment for future action by any department or by the Federal Government should be taken from any recommendations contained herein.

This report is to be considered as a background working paper and no effort has been made to edit it for uniformity of terminology with other studies.

TABLE OF CONTENTS

REGULATION

INTRODUCTION

This report has been produced with the aim of combining with the reports of personnel and consultants working within the "Privacy and Computers" Study set up by the Department of Communications and of Justice. In particular, this report is intended to be read with the report of Claude Fabien, and these reports deal with such matters as the formulation of appropriate definitions of data banks within Canada, rules for the operation of such data banks and the relationships between them and file subjects, and finally, possible regulations leading to and controlling professionalization and for self-regulation of the data processing industry.

The underlying goal of the considerations described above is the protection of privacy, and, accordingly, it is necessary to consider the term. However, since others are to examine this concept in more detail it is sufficient here to refer with approval to a statement attributed to a distinguished panel by Dr. Kenneth Cheng:

> The right to privacy is the right of the individual to decide for himself how much he will share his thoughts, his feelings, and the facts of his personal life. It is a right that is essential to insure dignity and freedom of self-determination.[1]

The final introductory function is the need to briefly describe the problem which we are attempting to deal with in this report. Although much of the danger from data accumulation is hypothetical in view of the infancy of the technology in some areas, certain current developments may indicate what looms ahead. First of all, we may begin to contemplate the consequences of the computer's ability to gather in one place data which was formerly stored separately. One commentator stated:

> What we seem to have done is rely on inefficiency to protect our privacy -- to protect us from these particular dangers -- and we suddenly realize that we can no longer do so . . . We are susceptible to injury by anyone who wants to work hard enough to do so, and this will continue to be true unless we take steps to discriminate among the <u>kinds</u> of information that are gathered and stored.[2]

Data from a great many private sources such as banks, insurance companies, and employers, as well as that from government agencies, could conceivably be accumulated in one file about an identified person. Thus Jerry M. Rosenberg asserted that a computerized system containing data for every man, woman and child in the United States, received from any form or questionnaire they had ever filled out, is within current capability.[3] Furthermore, the greater capacity could easily create a greater hunger for data. Prof. Arthur Miller warns that:

> In accordance with a principle akin to Parkinson's Law, as capacity for information-handling increases there is a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, motivates the collection of data pertaining to a larger number of variables.[4]

On the other hand, the centralization of information may make it feasible to employ greater technical and procedural protections against harmful disclosure of privacy-invading data. This is the optimistic side of the coin.

Another feature of computer technology is the development of remote access time-sharing systems enabling a central computer to be employed simultaneously by more than one user from different remote stations. This arrangement involved the communications media; indeed it has been forecast that by the late 1970's the telephone system communications will be about evenly divided between voice and data transmissions.[5] The effect of this is that "wire tapping" or transmission interception becomes a problem for privacy protection of computerized data. An illustration of the danger was provided when students on a project at M.I.T. once tapped into lines carrying government data from Strategic Air Command.[6] The consequence of this for the policy-maker is that privacy policies designed to protect computerized data must be integrated with communications policy and the criminal law.

The current state of the technology enables us to foresee other problems as well as those of personal data accumulation and communications interception. The abbreviated data placed into the computer may be incomplete or may contain errors or distortions. This danger is magnified by the tendency to place greater "dignity" or "authority" on computer-processed data. Furthermore, the computer personnel themselves may, by carelessness or wilful misconduct, help to bring about harmful disclosures of personal or commercial data, especially when the storage capacity of the computer increases the reward for the successful saboteur. Compounding all of this is the inadequacy of the current law. The absence of privacy legislation in most of Canada, the truth defence to a defamation action, and the uncertainties in the application of doctrines of negligence, confidentiality, or proprietary rights can be formidable barriers to the party injured by a disclosure of personal data. Stronger means are needed to protect him from the privacy problems created by the new computer technology.

DEFINITION AND SCOPE

In considering the appropriate perimeters for federal activity in this area there are two key concerns -- jurisdiction under the B.N.A. Act and definition of the subject matter to be controlled. It is expedient here to comment briefly on the first issue even though others on the Task Force may be dealing directly

with constitutional matters. In regard to licensing of information systems, it appears that no federal jurisdiction exists unless the system involved is one within the federal government or is one with sufficient extra-provincial links to make the enterprise itself a subject for federal jurisdiction. Of course the federal power in section 92.10(c) of the British North America Act to declare undertakings to be works for the general advantage of Canada is available and is exemplified by licensing under the Canada Grain Act,[7] but the infrequent use of this power in modern times appears to indicate that this could be unsatisfactory. There is, however, strong case law to support the assertion that federal jurisdiction over an interprovincial operation extends to regulation of the rights and obligations of its employees.[8] Federal jurisdiction over criminal law provides a basis for penal sanctions which could be imposed on the system or operator, but clearly does not justify licensing and regulatory provisions. Matters of civil liability, such as those concerning strict liability or contract, are clearly matters of provincial concern as indicated by the enactment of privacy legislation in Manitoba and British Columbia. Thus an effective over-all policy of privacy protection for computerized data requires close co-operation between federal and provincial governments.

There is also a need for international co-operation, or at least a concern for the extent of control in the United States. It would be senseless to so regulate the computer industry in Canada that almost all of its operations are transferred below the border. The situation also raises problems for the effectiveness of the regulations themselves. As Professor Lawford stated:

> Yet, if either the United States or Canada enacts legislation to protect privacy, there are dangers that the legislation can be avoided by utilization of international boundaries. Thus, a Canadian legislature might well enact a law requiring that any credit bureau provide an opportunity for persons to inspect files concerning their own credit ratings. Could the credit bureau avoid this law by simply moving its operation to the United States, and providing a telephone service to Canadian subscribers?[9]

International co-operation would thus be of valuable assistance in the creation of effective protections for privacy and controls over international communication of personal data.

Any attempt to legislate concerning the operation of information systems cannot be undertaken without a definition of the term to set the context and limits of control. The absence of source material on the definition and classification of the term makes the task more difficult, but does not make it any less essential. Perhaps here we can provide a starting point for discussion of the definition and classification of information systems by dealing briefly with possible approaches, and then suggesting why a classification based on the type of data stored may be best.

At the outset, we would tentatively suggest the following three factors as criteria for evaluation:

1) the definitions should separate the innocuous systems from those with high potential for privacy deprivation;

2) the definitions should set clear limits to enable those wishing to operate or regulate information systems to determine the application of legislation to a given system;

3) the definitions should have sufficient flexibility to cope with new developments in information storage.

With these criteria in mind, we will look at approaches based on size, purpose, basic unit or type, and data stored.

A definition based on the number of bits of information stored, or the number of persons about whom information is stored, might provide clear perimeters but would certainly fail to separate innocuous from dangerous systems. Thus a computerized telephone directory for a large area might fall within its limits while records of psychiatric or personality reports on a small number of people might not. Furthermore, technological progress would likely require constant revision of any quantitative limits.

Another means of definition and classification is that based on the purpose for which the information is stored. Thus Professor Alan Westin, in describing the data systems of the 1960's to the Subcommittee on Administrative Practice and Procedure of

the Committee on the Judiciary of the United States Senate, on February 6, 1968, noted five types of private data centers and three types of public data centers. The problem here is that, aside from questions of clear distinctions, the purpose of the data storage, while it relates to the types of data stored, does not in itself establish the sensitivity of the data. Thus a public data bank to assist in law enforcement may or may not go beyond public conviction records to include data on persons of unusual political loyalties; a data bank to assist in the development of land use policy might or might not include personal or financial information about land owners and a "computerized employment service" might or might not go beyond qualifications and experience to include credit data or confidential employers' references. Finally, it might be difficult to determine in advance the purposes for future data banks.

A common distinction on the type of data bank is that between "statistical" systems and "intelligence" or "individualized" systems.[10] The problem with this broad distinction, as the Gallagher Committee noted, is that statistical systems can be just as dangerous because they must retain individual identifications on data in order to make meaningful additions to the data or correlations among factors.

A similar approach which deals with basic data units is that raised by Albert Mindlin, Chief Statistician, Government of the District of Columbia, noted by the Senate Subcommittee on Administrative Practice and Procedure indicated above.[11] He distinguished among real property data systems, geographic systems, personal systems and family systems. While this could separate some of the innocuous systems, it would not go far enough by using such a simple criterion as the individual basic data unit. Both telephone directories and character investigation reports are "person systems". The ability of a system to separate data about an individual may be used as one essential characteristic of those systems to be regulated, however, although even here a commentator has noted a need to protect "proprietary data" of groups of businesses.[12] Whether such protection is later required may depend on the usefulness of the law of contract, with or without compulsory standard terms, in this area.

Another means of classifying information systems would be on the basis of the particular data stored. Professor Westin comments:

> . . . we need in our legal system some procedure for classifying information into various categories and distinguishing the rights to use of such information according to such classifications. For example, personal information could be divided into matters of public record that are expected to be open to virtually everyone; confidential information that is given in trust to certain individuals or agencies with the expectation of limited use; and security information which is either given under the expectation of complete non-circulation or which contains derogatory information about individuals that has been obtained by physical and psychological surveillance. Different standards must be set for the receipt, storage, and circulation of such different classes of information.[13]

Our suggestion is that there should be a breakdown of types of individual information, on a basis similar but not identical to what Westin gives by example, into three groups. These could be:

a) Matters of general accessibility. This would include such matters as name, residence, social security number, age, sex, employment, marital status, immediate family, registered property ownership, registered chattel mortgages, bills of sale and liens, bankruptcies less than 14 years old, court records with general public access (perhaps with a restriction as to age of record), membership in clubs and associations, education, and any other matters, except those indicated below, freely obtainable by persons with no special qualifications. The idea behind this grouping is that it is pointless to regulate information systems which have records which can be readily obtained from public sources.

b) Confidential information. This would include such information as actual or estimated income, bank account records, medical records, outstanding credit obligations, paying habits, employment references, private character reports, writs or criminal charges pending, etc. A qualification might be feasible whereby information freely given by a person with informed consent to unrestricted circulation is not confidential.

c) Sensitive information. This would include such information as police reports, results of personality tests, family counselling records, income tax returns, census returns, information subject to solicitor-client privilege, juvenile criminal records, and criminal records of a specified age.

Such a system is designed to distinguish the dangerous records from those with minimal privacy implications, to provide clear delineation of classifications and to include future records of personal data not presently stored systematically. The major

objection to such an approach appears to be the assertion that the sensitivity of data depends upon its use. Thus Professor Miller reports that the House Committee on Government Operations rejected a single scale of confidentiality to rate every report received by the Government because they believed that ". . . the imposition of a uniform scale would obscure the fact that 'the sensitivity of a given document is not intrinsic, but varies with the relationship between the agency gathering the data and the agency receiving it.'"[14] Despite this, however, other authors besides Westin call for the categorizing of information.[15] We have already noted the problems encountered by focusing on purpose as the criterion for classification. Accordingly, it is hoped that the force of the objection indicated above can be mitigated by other limitations on the operative definition relating to circulation or consent, as set out below.

To illustrate how such a classification would operate, we can consider the information commonly recorded by credit bureaus as indicated in "Credit Bureau Policies to Protect the Right to Privacy" developed by the Associated Credit Bureaus of Canada. The information could be classified as follows:

> General accessibility -- name, age, place of residence, marital status; family, place of employment, judgments (not writs) concerning consumer debt, non-responsibility notices, registered chattel mortgages, and convictions under provincial statute or for criminal offences (provided the latter were not outdated, concerned an adult, and were freely obtainable).

> Confidential information -- previous places of residence, previous places of employment, estimated income, paying habits, outstanding credit obligations, writs concerning consumer debt, and conditional sales contracts (unless publicly registered).

Thus the typical credit bureau would be classified as a system containing confidential information; a telephone directory, on the other hand, would be one with information of general accessibility.

The above definitions could then be used as perimeters for federal governmental legislative action within its jurisdiction. A "data bank" or "information system" subject to regulation could then be:

> . . . a data storage system containing confidential or sensitive information about a specific individual identified by name or by means through which the name may be readily obtained.

This would include systems which use social security numbers or other traceable identifications. An "information system operator" could then be:

> . . . a person who retrieves individualized information directly from the information system rather than from another person or source.

The "owner" of the system could also be set out for the purpose of assigning strict liability. The policy makers might also wish to confine the controls to the computerized data systems, although this would have a detrimental effect upon development of efficient systems.

Further exceptions are also called for in order to avoid unnecessary control of records owned by the body storing them, those with restricted access, or those to which an individual consents. The principle of focusing upon systems which "externalize" information, suggested by Professor Gotlieb at the Queen's Conference, could be included in the scheme.[16] Thus the regulation scheme could be specifically stated to be non-applicable to systems containing:

> . . . confidential information for which either
> (a) the free consent of the subject to its unrestricted accessibility has been obtained; or
> (b) the information was voluntarily obtained from the subject and access to it is restricted (excluding requirement of law) to the person, association or agency collecting the information, employees of such person, association or agency, or others whom the individual subject was informed beforehand would receive it.

These last provisions require some comment. The "consent" criterion is not accepted by all of those who comment on the privacy issue. Mindlin discussed the issue by posing a question concerning government statistics:

> Should the permission of an individual be obtained before creating an individual integrated record for him within a statistical data system? No. This would be prohibitively expensive and so cumbersome as to effectively block the development of a system. Also it would be meaningless. How can an individual applicant for a community service understand or foresee the implications, uses, and limitations of his record in the system? Also how much 'freedom' would, say, a welfare client feel he has in this matter?[17]

Of course, in the scheme proposed here the absence of consent would not prohibit the storage of the data, but would only subject the system to regulation. The problem of freedom of consent is a serious one, but it is hoped that the use of the term "free consent" could eliminate situations where provision of a needed service is conditional upon consent to data accessibility. Furthermore, officials should be encouraged to indicate other users of the information wherever possible. With proper qualifications, the consent criterion can be feasible. Karst, recognizing some of the difficulties involved with the concept, stated that:

> Almost every such fact, however personal or sensitive, is known to someone else. Meaningful discussion of privacy, therefore, requires the recognition that ordinarily we deal <u>not</u> with an interest in total nondisclosure but <u>with</u> an interest in selective disclosure. Our concern is with unauthorized access to the files, and so we begin with an assumption, built into our definition of privacy: consent by the subject of the file excuses the disclosure of information about him.[18]

The second point is that care must be taken to ascertain the existence of a data transfer. Professor Miller notes that we are not dealing only with manual transfer of manilla folders, but are often concerned with computer systems where a record may be fed directly by machine interface and be duplicated so that the original remains with the collecting agency.[19] Such operations should be considered data transfers unless within the same agency or government department.

Further use may also be made of the classification. Ideally, a statute would establish a duty of confidentiality in relation to confidential information with a tort remedy for its breach, or strict liability for improper disclosure of confidential or sensitive information, but this is undoubtedly beyond federal jurisdiction, except possibly in the case of federal government records, in view of the general privacy statutes of several provinces. Similarly, in the area of sensitive information, the data subject could have a cause of action, without proof of damage, against anyone retaining or transfering such records without either (a) the free consent of the individual subject (here consent could often be implied as, for example, where a family counsellor keeps records of those coming to him voluntarily), (b) express statutory authority, or (c) a court order from a designated court. Law enforcement agencies could be given specific exemption for police records. In addition

there could be other records, such as that of information obtained by illegal surveillance or classified miliary information, which could only be obtained under express statutory authority, subject to summary conviction for violation.

The flexibility of the classification system would, it is submitted, be enhanced by the general criteria which could include some information not yet systematically recorded. This alone, however, would be insufficient. It would likely be best to encourage regular study and amendment of the classifications either by regulations (with the disadvantage of restricted publicity) or legislative amendment. This should be the responsibility of the regulatory agency proposed elsewhere in this project which should have the initiative and discretion to propose and publicize such changes.

LICENSING AND CONTROL OF INFORMATION SYSTEMS

The licensing of information systems and the corollary power to refuse to grant a license is one of the possible means for the federal government to deal with its responsibility to ensure that personal privacy is not sacrificed by the operation of inter-provincial or international information systems. It is submitted here that a government-sponsored but substantially independent agency, which could possibly include representatives from the information

system industry, should exercise responsibility for licensing and policing the information systems. The agency would have the power to establish technological and procedural license requirements for any given system, and to deny the ability to operate to any system which could not be certified satisfactory in the maintenance of the standards. The licensing scheme would be designed to deal with the private sector of the industry, although the same agency could exercise responsibilities in the supervision of government operations (to be discussed in a later section). The disciplinary function could operate in cases where public complaints as well as agency inspection reveal sub-standard operation.

Provisions which place such powers in the hands of a regulatory body can only be justified where the public interest and the need to protect public health, safety, and morals is sufficient. The present concern for protection of privacy may very well indicate that we have reached this point. The agency would not only eliminate systems with insufficient consideration for privacy, but would also serve the public as an additional avenue of redress for malpractice. Another challenge to such provisions could be on the grounds that they grant excessive power to a government body. However, despite the efforts of groups like the Associated Credit Bureaus of Canada to develop advanced policies respecting the right to privacy, it is doubtful that the industry itself could exercise sufficient powers

of sanction to enforce the rules or could achieve sufficient independence from the operating system to inspire public confidence and acceptance for impartiality. Furthermore, the role of ethics, a key to self-regulation, may be less significant in a commercial setting with standardized product and impersonal "staff"[20] and self-regulation on the basis of ethics would be more effective in relation to the operators of the system than for the system itself. It appears preferable to meet the objection to "Big Government" by seeking to make the regulatory agency more independent of other operating agencies. Further protection for the industry would be a limitation of the agency's supervisory and disciplinary role to matters involving protection of privacy and, by denying to the agency power to limit the number of licenses on economic grounds or to regulate charges and wages, to leave control of the industry's economic environment to the private enterprises themselves.

Legislation to establish a licensing scheme should have clearly defined objectives, perimeters of operation, and grounds for disciplinary action. It should be clear that no information system within the defined group can operate without a license from the agency and there should be no doubt that the agency has power to renew, revoke, or suspend licenses. Commentators have indicated that unqualified discretion with the ability of an agency to set and alter its own standards, or even operate without pre-established

standards, increases vulnerability to external pressure and adds to uncertainty on the part of those subject to the agency's jurisdiction.[21] This problem may be particularly difficult in the area of technical requirements for certification where each system may have to be judged according to its data, circulation of data, data use, and other facts, but hopefully experience in the area can lead to development of guidelines while standards may be more clearly set out in other areas. The authors of the McRuer Commission Report favoured setting out objectives and policies in legislation to assist in establishing standards, and concluded that:

> 'Complete impartiality and integrity' of the administration of a licensing policy will be assisted and enhanced if the legislature expresses as far as possible 'the purposes envisaged by the statute' and the 'considerations pertinent to the object of the administration.'[22]

In light of the above, legislation in this area should express the view that information collected from individuals is not always a separate commodity concerning which the individual subjects have no further rights or interests. It should indicate that the purpose of the provisions below is to protect the individual subjects from unreasonable disclosure of information about them which violates their right to privacy.

It is now appropriate, with the above comments in mind, to examine the licensing aspect of the agency's operation. The license should be issued for a limited period of time -- 2 years might be a satisfactory period, depending upon what experience and study reveals best - with procedure for renewal. The following features merit specific examination:

1) Certification

The expert staff of the licensing tribunals and those on the tribunal itself would be responsible for determining the technological and procedural requirements for a license in each separate case. Determination of the requirements should take into consideration such factors as the sensitivity of data, the circulation of data, the uses of the system, the cost of the protections for the system owner and those using it, the effectiveness of each protection in the context of that particular system, and past performance of the system. Although this project is not intended to deal with technical protections, some of those commonly cited can be referred to. Some of the technological features are the various identification systems with codes, wafers, "answer back", etc. for remote access terminals, the coding or scrambling of data with limited access to codes or descrambling keys, designing a monitor or control program with "privileged instructions" to provide the only means of altering the monitor program,[23] and programming computers to reject output instructions which enable identification of the data subject due to the small sample or other means.[24] Procedural means are also available. In "statistical" systems, for example, it is possible to separate the material giving the identity of the subject from that which contains the impersonal data, and access to the former can be more limited. Other procedures include the ranking of data hierarchially on a sensitivity scale with only trustworthy staff having access to the most sensitive data, the maintenance and review of a log or audit of data retrieval,[25] control of physical access, and ethical criteria in personnel selection.

2) Expert participation

Expert staff would be essential to enable the licensing authority to assess appropriate protections and inspect the systems in operation. Aside from the staff, some members of licensing tribunals should have expert qualifications to enable them to deal responsibly with technical arguments advanced by licensees.

3) Inspection

The agency staff should inspect information systems to ensure that certification standards are maintained, and should institute proceedings for license revocation for violations which are not corrected.[26]

4) Review

A regular review with a view toward license renewal should be made when the license term is due to expire. In the event of a major alteration of a system, as determined by agency staff, a new license should be required. Provision could be made here for license determination on the basis of proposed change so that systems owners are less likely to undergo expensive alteration only to meet with a license denial.

5) Conditional licenses

The addition of conditions in the grant or renewal of a license can be a creative regulatory tool, but the failure to put limits on this power could open the door to unqualified discretion.[27] Thus it is suggested here that it should be possible for a licensing agency to attach conditions to the grant or renewal of a license, but only if the condition sets out an objective course of conduct for the licenses. Vague conditions with a general requirement that future conduct be acceptable to the agency should be avoided altogether or used only where a re-hearing is set within a specified time.

6) Financial responsibility

Licensees should be required to show proof of ability to compensate those who may suffer from their information system. Two methods appear appropriate. One would be the posting of a bond of an amount to be determined. This is not a novel requirement in Canada; the Canada Grain Act, for example, requires the furnishing of a bond with proper sureties or other security from a licensee.[28] Another means is indication that the licensee has proper malpractice insurance. One writer, while discussing a national medical data center, considered forbidding the writing of malpractice insurance for criminal or civil losses related to privacy considerations.[29] He finally commented, however, that:

> It might be assumed that lack of malpractice insurance protection will deter practitioners from flirting with privacy breaches by exposing their personal resources to legal judgments. Many would-be violators probably would not be influenced by such a prospect and might have such marginal financial resources, as well as marginal ethical resources, that they would not be able to compensate participants they injured.[30]

It is submitted here that the minimal deterrent effect, coupled with the need to compensate persons suffering injury, make it advisable to allow such insurance. Malpractice insurance and bonding are valuable instruments in the operation of a strict liability scheme, which will be discussed below.

7) License limitation

One of the major objections to licensing boards, notably those governing professions and occupations, is the danger that boards with representation or control from the subject group will govern in the self-interest of that group.[31] Unrealistic entrance requirements are used to limit competition and resist modern advances. Accordingly, it is suggested here that, at least until the industry can satisfactorily show serious harm to the public resulting from open competition, there should be no limits on the number of licenses to be granted. Great care should also be taken to ensure that the technological, procedural, and financial responsibility requirements are not unreasonable with the result that they discourage entry into the field.

8) Licensee rights

No licensee should be denied a license or penalized without full opportunity to plead his case, and decisions should be in writing with reasons set out as completely as possible. Appeal provisions should be available. These protections and others will be discussed after a consideration of the disciplinary function of the agency.

The agency should also be responsible for disciplining the information systems to ensure that respect for privacy is maintained. Its jurisdiction should include all information systems handling confidential or sensitive personal information and failure to have a license, rather than acting as a barrier against agency action, could in itself constitute a violation where the system falls within the definition set out above. Most of the disciplinary function should consist of hearing complaints and dealing with instances where licensing staff believe that proper standards are not being maintained. Several features bear comment.

1) Seeking out complaints

Licensing staff should consider it their responsibility to publicize this means of redress so that justified complaints can reach the agency. Co-operation should be sought from bodies such as newspapers, the ombudsman, and Better Business Bureaus for referral of complaints. It might be advisable to place a duty on the industry operators themselves to report violations in order to improve detection of sophisticated violations while reducing the stigma on the informer,[32] although this works best for dealing with individual computer operators as distinguished from the information system.

2) Independence

The disciplinary bodies should be an entirely separate wing of the regulatory agency from the licensing bodies. It is hoped that this will enable prosecutions to be conducted by the licensing staff without there being unity of prosecutor and judge. Hopefully the restriction of liaison to the highest levels only and the separation of working space can avoid the danger of excessive co-operation between adjudicating and prosecuting.

3) Specification

The expression of specific acts for which revocation or suspension of a license may be justified would assist in the clarification of standards for disciplinary action, and would provide guidelines for evaluation under more general terms like "insufficient provision for privacy protection". While such a general term will likely be necessary to deal with unforeseen violations, it could follow the setting out of specific actions constituting grounds for discipline, and could be expressed to require the involvement of "similar" factors. Examples of such actions could be the storage of confidential or sensitive personal data without a license, the unauthorized disclosure of confidential or sensitive individualized data, failure to maintain certification requirements, refusal to verify or correct erroneous information when requested to do so, or refusal to permit access to a person's file without valid grounds (such as previous access within the year, cases of medical records or references which should be withheld, etc.). The strong possibility of accidental violation or of third party misconduct makes it advisable to consider making intention, recklessness or negligence essential elements for any disciplinary action beyond a reprimand.

4) Expertise

Each disciplinary board should have one or more experts to provide responsible evaluation of technical or procedural arguments. In another context (that of stockbrokers in the United States), Philip J. Hoblin Jr. noted the value of experts when he pointed out that:

> Generally brokers prefer arbitration when they are right and courts when they are wrong. It is difficult to confuse an arbitrator of long experience in the securities business, while the technical aspects of securities transactions often prove incomprehensible to persons outside the industry.[33]

5) Penalties

The penalties available for enforcement should be clearly set out and should range from a reprimand to a revocation of license. As noted above it may be desirable to restrict the use of the latter sanction to cases involving wilful or reckless action, while a suspension or fine should require intention, recklessness, or negligence. A limit should be placed on the maximum length of time for suspension (perhaps one year) and this should not be longer than the time period after which a licensee whose license has been revoked can apply for a re-hearing and return of the system's license. Provision should be made for a return of license upon reconsideration where the owner whose license has been revoked wishes to sell his operation and the new owner shows proof of a desire to improve performance in the privacy field. Fines should be available within set limits, and a decision would be required on whether funds so received should go toward agency expenses, an indemnity fund (perhaps to pay costs for those who successfully defend themselves against complaints) or the public treasury. Civil remedies for injured persons and criminal sanctions for serious abuses involving fraud, forgery, or other devices should not, of course, be restricted by agency operation. Furthermore, it might be advisable to provide a civil remedy, as well as the availability of a writ of mandamus, for persons injured by unreasonable refusal of the agency to act on a complaint.

6) Licensee rights and appeal

The right to a hearing to respond to proposed disciplinary action should be legislatively guaranteed, and appeal rights should be set out. This is further discussed below.

Legislation dealing with the licensing of information systems or regulation of information system operators (as defined above) should also attempt to provide adequate safeguards for the rights of those subject to the agency's jurisdiction. A valuable discussion of this general issue, with particular reference to the licensing of individuals, is provided by the McRuer Commission Report, Volume 3, Report No. 1. The comments below are intended to set out briefly some means of protection which bear consideration.

1) Right to a hearing

While an agency official should be authorized to give out licenses in the absence of any complaints or allegations, no candidate should be denied a license or no operator should be penalized without the right to a hearing before the licensing body where he can present his side of the situation. There are two main factors to be considered in determining whether such hearings should be open or closed -- the danger on the one hand that the secrecy of such hearings can increase the ability of the agency to exert unnecessary arbitrary pressures,[34] and, on the other hand, the prejudicial effect of public disclosure of unfounded allegations. Accordingly, it is submitted that the licensee or operator should be entitled to choose between a public or closed hearing. Furthermore, it should be specified that the decision must be based only on matters disclosed at the hearing.

2) Notice provisions

A licensee or operator should always be notified of any complaint which has been made about him, and he should always receive sufficient advance notice of any hearing which will concern him. In the United States, section 9(b) of The Administrative Procedure Act goes further and provides, in part, that:

> Except in cases of willfulness, or those in which public health, interest, or safety requires otherwise, no withdrawal, suspension, revocation or annulment of any license shall be lawful unless, prior to the institution of agency proceedings therefor, facts or conduct which may warrant such action shall have been called to the attention of the licensee by the agency in writing and the licensee shall have been accorded opportunity to demonstrate or achieve compliance with all the lawful requirements.[35]

It is worthwhile to consider providing licensees and operators under the legislation herein considered with a similar provision, provided that the exception is sufficient to take account of the possible severity of a violation and/or difficulties in detecting violations. In less serious cases, advance notice and opportunity to adjust could perform a valuable service. As a Note in the Harvard Law Review comments:

> When the licensee is not conscious that his activity is improper, either because he is unaware of the agency regulation or because his interpretation of the regulation is one of several among which the agency has not yet chosen, then any violation is probably the result of ignorance. The section is intended to protect licensees from the harsh sanction of revocation for such excusable misconduct. Notice provides the means by which the agency informs the licensee of the regulation or clarifies it by interpretation, and opportunity to comply offers him a chance to demonstrate good faith by future conformance.[36]

3) Written reasons

A requirement that all adverse decisions be accompanied by written reasons has the benefits of reducing the temptation to make a decision for improper motives and of facilitating the conduct of any subsequent judicial review or appeal. The decision should only be based on matters expressed in the written product.

4) Publication of standards and reasons for action

The agency should be responsible for seeing that any regulations or policy statements which it makes are well publicized among those who operate centralized information systems. The agency should also promote the publication and circulation of any code of ethics devised by the operators themselves. And, thirdly, the provision of written reasons for disciplinary action, plus the circulation of a list indicating conduct for which disciplinary action has been taken, should also be undertaken. These activities are necessary to enable the conscientious licensee or operator to know that conduct of a certain nature is or is not acceptable.

5) Appeal and judicial review

The new Federal Court Act deals with the disposition of such appeals. The Trial Division would appear to have jurisdiction to issue injunctions, writs and declaratory reliefs against the federal agency by section 18, while under section 28 the Court of Appeal has exclusive jurisdiction to review and set aside non-administrative orders of a federal board for abuse of the rights of natural justice, ultra vires or refusal to exercise jurisdiction, error of law whether or not it appears on the record, or capricious and unsubstantiated and erroneous findings of fact. Supreme Court jurisdiction is dealt with in section 31, and does not include decisions based on fact alone unless leave is obtained. Should the exercise of appeal rights come to place an unwarranted burden on the Court, it may be advisable to restrict appeals based on the final decision to those cases where revocation of license or serious disciplinary measures have been ordered.

6) Rehearing

A licensee whose license has been revoked should be allowed to reapply after a specified time on the basis of evidence of rehabilitation. A hearing would be necessary to determine the disposition of the application.

7) Impartiality

Should it be determined that industry representatives will sit on disciplinary boards, a potential problem could arise in regard to impartiality. In the case of disciplining an individual operator it should not be too difficult to find a representative who is unacquainted with the person called before the board and does not share the same employer. But where a licensee is being considered for disciplinary action it could be difficult to find someone from the industry who would not be suspected of partiality on grounds of employment or competition. Government information systems operators may or may not have sufficient disinterest. Hopefully these problems can be solved -- if not it may be necessary to do without industry representatives on the board in certain cases.

REGULATION OF GOVERNMENT INFORMATION SERVICES

The above discussions dealt with control of private information systems such as credit bureaus or others falling within the definitions. Since there is no desire to exclude governmental records from controls designed for privacy protection, it seems appropriate now to discuss control over federal government records. It may be feasible to subject all information systems of governmental agencies to the same licensing requirements but make exceptions in the case of Statistics Canada, on grounds of its statutory powers, and operating traditions, and in the case of any other governmental records such as law enforcement records where it is totally inappropriate to consider a revocation or suspension of license. The exceptions should be specifically spelled out in the definitions, and the statute could go on to set out policies for such records. However, since the Senate has just considered a new Statistics Act,

there is little necessity here to engage in detailed discussion. It will suffice to deal briefly with general policy and with the possible role of the same regulatory agency that deals with private records.

Much has been written to promote the creation of an agency within government, but independent of any operating agency, to retain and control governmental records.[37] The agency referred to in the previous section, which could possibly report to the same Minister as Statistics Canada, could perform a regulatory function in the governmental area as well. Policies in this area would have to recognize that government agencies involved in such activities as law enforcement, social insurance, or urban renewal simply must be allowed to keep detailed records if they are to function effectively, and that information exchanges among some of these is a "nonreversible historical fact" in some areas,[38] especially since this prevents the need for original respondent to supply the same information again. But this should not be allowed to prevent a regulatory agency from seeking a balance between governmental needs and individual privacy needs and to step in to prevent collection of unnecessary data, unnecessary transfer of personal information, or use of improperly obtained data. Use of "non-statistical" data -- data where the individual respondent's identity is known -- should be avoided where possible, and representations made to a respondent concerning limited use or circulation of information should be respected.

In light of this policy, the independent agency could exercise supervision of data use by operative government agencies in four major areas. The over-all scheme bears resemblance to that described in an American article,[39] but some of the ideas have been discussed by many commentators. The four areas merit separate comment:

1) Determination of whether new data ought to be gathered

This function could be carried out by Statistics Canada itself or by the independent agency. Professor Miller has described some of the requirements which should be met before new data can be gathered.[40] Appropriate requirements include: 1) a demonstration, with specific proof, by the agency seeking the data that there is a clear and significant need for it (this would include description of the use to be made of it); 2) a showing that the information was not available elsewhere from other accessible federal records, records of other government levels, or private sources; 3) a finding that the sample group is neither too large nor too small; and 4) a demonstration that the questions to be asked are not intrusive or violative of privacy. The onus should be on the agency seeking the records to demonstrate the above.

2) Consideration of whether access to data should be given to another agency

In this case, the agency would decide whether data gathered for or held by one government agency should be made available to another. Factors such as those given above would be relevant here with emphasis on whether there is a need for the data, the proposed use to be made of it; the sensitivity of the data; and any representations made to the respondent or obligations imposed on him when he supplied the data.

3) Destroying obsolete information

Statistics Canada, individual government agencies and the regulatory agency itself should all be encouraged to destroy or at least remove from active file all personal information which has become outdated. It may be feasible to remove identification indicia and retain the data only in statistical summary form. This would promote both efficiency and respect for privacy.

4) Supervision of employee conduct

The agency should be concerned to see that government employees at all levels who violate privacy regulations are properly sanctioned. There is no reason why government information systems operators should not generally be subject to the same sanctions of civil and criminal law, as well as the same regulation of individual operators, as those operating outside government. Additional sanctions, such as those in the Statistics Act, may continue to be used.

Hopefully the above precautions can help to preserve a balance between governmental information needs and individual needs for privacy.

FOCUS UPON OPERATORS

A scheme to protect privacy in information systems would be seriously weakened were it not to deal with the operators of the system. These persons are distinct from the owners of the system and are, as defined above, those who obtain the personal data directly from the information system. This project will consider whether professionalism and self-regulation can act as acceptable controls upon those people. The conclusion is that the federal government should encourage self-regulation by the operators of a government-sponsored code of conduct.

The professionalization of the information systems operators would be almost certain to enhance respect for privacy and reduce the need for extensive government control. As Professor Miller put it:

> The inculcation of a sensitivity or professional commitment to the values of personal privacy and the dignity of the individual may provide a far more effective long-term check on the custodians of personal information. Moreover, it may be that the basic philosophical question -- what are the duties and responsibilities of those who handle personal information affecting their fellow man -- is as much an ethical dilemma as it is a legal issue. If so, perhaps it is best left for regulation by the practitioners of the art in the first instance.[41]

Furthermore, the professional group may be a very powerful influence in favour of acceptable conduct; F.A.R. Bennion states that, "The conduct of barristers, for example, is much more affected by what their brethren would think than by what is written in the handbook on etiquette at the Bar".[42] It is difficult to determine, however, just what constitutes a profession and it is difficult to assess just where information systems operators fall, especially if the group goes beyond those who handle computers storing personal data. Lord Balerno believed in 1969 that computer operators had become a "discrete profession".[43] Other factors may work against professionalism. As Frymeer noted in relation to education,[44] the "line of authority" situation wherein the individual is subject to a hierarchy of supervisory staff or bodies may inhibit the development of co-operation

among professional peers and create a tendency to deal with disciplinary problems through the authority chain with no reference to the profession. Also those operators who work more often with the record-keeping system than with the public will be more likely to place added value on the efficiency criterion and less on that of personal service.

In light of this uncertainty, it is submitted here that the federal government ought to do its best to encourage the development of an information system operator association. The emphasis upon the duty of an officer of Statistics Canada and the taking of an oath set out in the Statistics Act hopefully indicates that a tradition in favour of personal responsibility for privacy protection already exists; perhaps the staff of Statistics Canada could provide the nucleus and incentive for an effective association. Experimentation is undoubtedly necessary in this area. In the final analysis, the onus lies on the operators themselves to create their own body which could help them secure a stronger role in the control of their group and reduce that which the government may have to undertake at the outset.

The comments on professionalism provide a logical introduction to the next consideration -- the advantages and disadvantages of self-regulation. Of the disadvantages, one of the most common complaints levelled at American licensing boards controlled

by an occupation or profession is that the interests of the group allegedly controlled are given priority over the public interest. Thus, on the pretext of protecting the "public interest" in proper standards, the group may control entrance into their numbers in a manner which reduces competition, provides a shortage of trained personnel, resists the advances of new techniques of practice or training, and provides protection for the group against public complaints.[45] The McRuer Commission in Ontario appeared to share similar concerns, and stated that arguments for state control are stronger where the bodies involved are not professions in the traditional sense but their members are more trained technicians.[46]

Self-regulation also presents problems for the enforcement of standards. An American writer claimed that excessively decentralized bar association discipline facilities created problems of reluctance to proceed against prominent associates, absence of uniformity, delay in activating bodies which rarely sit, and absence of adequate staffing or finance.[47] Some of the criticisms have related to the field of privacy. Thus Professor Westin complained that ". . . the pressure of the new technology was so great and the sensitivity to privacy was often so slight among the professional groups that the 1945-1965 period was one in which ethical codes provided little control over immoderate use of surveillance."[48] Professor Miller noted that the Associated Credit Bureaus guidelines

reveal the concern of that group but are not binding and are "bountifully endowed with loopholes.".[49] Thus self-regulation likely possesses serious drawbacks in the privacy field.

Nevertheless, the advantages of self-regulation are attractive. In considering control of stock brokers, Harry N. MacLean noted three arguments for self-regulation -- expediency and practicality in light of the "ineffectiveness" of regulating directly through government on a wide scale, the benefits obtained from the expertise and experience of members of the industry, and the necessity to go beyond law and into ethics.[50] These are well summarized by a statement of Mr. Justice Douglas in 1938 that:

> By and large, government can operate satisfactorily only by proscription. That leaves untouched large areas of conduct and activity; some of it susceptible of government regulation but in fact too minute for satisfactory control; some of it lying beyond the periphery of the large areas self-government, and self-government alone can effectively reach.[51]

Another advantage would be reduced expense where members of the association or group supplied part-time membership for control bodies at lower remuneration. Finally, an interesting feature of the control by the Law Society in Ontario -- a fund created by a levy upon the profession as a whole to indemnify clients injured by their lawyers' incompetence -- might be set up by an association of information systems operators. Professor Arthurs claims that "When

claims on this fund mount, the Society will almost surely be driven to control or eliminate those whose incompetence creates a burden shared by the whole profession."[52] Self-regulation by information system operators can make a valuable contribution to the protection of privacy of personal information.

It is submitted here that the best policy would be to have a system of self-regulation of information system operators by the operators themselves on the basis of rules of conduct made or approved by the regulatory body of the federal government. The government involvement could be much reduced should a professional association of information system operators develop strong traditions and full membership.[53] The question of whether government supervision should be by the licensing or disciplinary wing of the agency would depend upon whether the government chose to determine very general policy only, in which case the licensing wing would be responsible, or wished to develop specific rules of conduct itself, whereupon the disciplinary group would be involved. The absence of a professional association would favour the second course at the outset. This supervisory role is well summarized by Professor Miller when he states that ". . . self-regulation must be viewed as a supplement to, and not a substitute for, policy determinations by other interested societal institutions as to appropriate minimum levels of privacy protection."[54]

This policy control could best be exercised through a code of conduct resembling a code of ethics. The following comments constitute suggestions for the content and enforcement of such a code.

1) Policy

Clearly no code can deal with all aspects of conduct on the part of those whose activity is being dealt with. Thus a preamble should resemble that quoted from the American Bar Association, Canons of Professional Ethics 1 of 1957, which reads

> No code or set of rules can be framed, which will particularize all the duties of the lawyers in the varying phases of litigation or in all the relations of professional life. The following canons of ethics are adopted by the American Bar Association as a general guide, yet the enumeration of particular duties should not be construed as a denial of the existence of others equally imperative, though not specifically mentioned.[55]

The code could then state that its purpose was to respect the privacy of personal information.

2) Entrance requirements

The code should state that no person can be denied the right to operate in an information system by the controlling body unless it is for one of the reasons set out below. This is designed to discourage the type of restrictions based on self-interest which were the subject of complaints about American licensing boards.

3) Character requirements

The suggestion in an American article that exclusion from a state bar association on character grounds should only be possible for psychological disorder or criminal record bears merit.[56] In addition the conviction or disorder should be one which bears sufficient relation to the activity involved. Thus a conviction for assault

should not ordinarily be grounds for denial of employment or membership in the association while one for embezzlement (indicating abusive use of confidential and important information) should be. The discretion to evaluate disorders or convictions within such criteria could be left with the controlling association. Thus a code might state that the following grounds alone could justify denial of the right to association membership and employment as an information system operator:

(1) prior violation of a statutory provision, rule, regulation or code concerning occupational or professional conduct, or a previous conviction at law, for conduct which indicates abuse of a confidential relationship, disrespect for a personal duty owed to a patron of the candidate's services, or unreasonable disclosure of confidential and/or personal information; or

(2) evidence supported by a duly qualified medical practitioner of a psychological disorder which could indicate an inability to respect the obligation to respect confidential and/or personal information.

Such provisions, rather than more general ones calling for "good character" etc., could also help to avoid the expense and unnecessary invasion of a candidate's privacy which investigation of other characteristics could involve.

4) Disciplinary powers

The association should have power to reprimand, fine, suspend, or deny admission to an applicant, similar to the licensing agency for the systems themselves. The licensing agency could put teeth into these powers by employing a certification requirement that all personnel handling confidential or sensitive information as information system operators must be members of the association. Violation of a rule should not of itself be grounds for civil liability to an injured party since this would discourage promotion of progressive rules by the association to keep abreast of new developments.[57] Such violation may, however, be available to constitute evidence of a cause of action.

5) Administration of discipline

Discipline should be by boards composed mostly of expert members of the association or occupation, with lay members experienced in adjudication, such as lawyers or arbitrators to act as chairmen. The experts would be able to deal with technical matters as well as allegations of negligence or professional misconduct. The licensing staff could be used, (at public expense) to conduct prosecutions or investigations although as information storage expands, it would be worthwhile to provide staff for the association at public expense. Co-operation should be sought with the licensing and disciplinary wings of the federal regulatory agency for referral of complaints. The permanence or number of the disciplinary bodies could be determined by the number of hearings required, with public (governmental) financial support should permanent disciplinary boards be necessary.

6) Specific acts

Specific acts for which discipline is required could be set out to provide clear guidelines for conduct. Appropriate acts could be similar to those given earlier as examples for the systems themselves. Hearings involving "negligence" or "unprofessional conduct" (discussed below) should be specifically required to concern conduct "similar" to that set out.

7) Negligence

Disciplinary provisions for negligence are justifiable when professional men are being judged by their fellows.[58] A similar provision might also be suitable for the code considered here provided the negligence resulted in unreasonable disclosure of information or posed a serious and continuing threat to such disclosure. The participation of experts on the boards should be of assistance here.

8) Unprofessional Conduct or Professional Misconduct

These could be grounds for disciplinary action. Here it is necessary to specify that the misconduct must be one indicating disrespect for the obligation to keep information confidential. It is likely not feasible to go beyond that. Thus, the McRuer Commission commented that:

> It may be impossible to stipulate in advance all the varieties and shades of activity which will be regarded as professional misconduct, and a general clause providing for discipline for 'professional misconduct' will always be necessary so as to allow the profession to take account of unforeseen types of misbehaviour.[59]

Here again, expertise and experience on disciplinary boards is important.

9) Protection

The protections described in a previous section for licensees and operators in general should be applied here.

In addition to this, the association might consider a levy upon the membership to provide compensation for persons injured by a member's default who have failed to obtain compensation elsewhere or for members successfully defending themselves against complaints. The decision whether to create such a fund or not should be left entirely with the association, and may depend upon the adequacy of civil remedies.

REGULATIONS AND DUTIES

There are other aspects of the storage of personal information which should be the concern of the federal government's regulatory agency. These could be dealt with by legislating duties for which the system itself would be responsible and by disciplinary action from the agency if the standards of performance are not maintained. Those duties which have been mentioned in considering "specific act" for discipline need not be mentioned further, but others which have received attention by others deserve brief mention here. Many of these relate particularly to credit bureaus because these are the existing systems with which there is some experience.

1) Identification

There should be a general duty not to use data which can be traced to an individual or carries an individual identity unless this is essential. For statistical records, the identification material should be maintained separately and linked to the data by code alone.

2) Access

There should be a duty to allow a person to have access to his file upon request as often as once a year, provided he identifies himself sufficiently. Since he would have to appear in person, there need be no cost for him. The major problem here is to prevent access to data which he ought not to see, such as confidential character records or medical records. A storage system should be entitled to refer the question -- whether access should be granted -- to the licensing agency free of charge for a determination at the time record storage is commenced.

3) Notification

There are opposing views of whether a data subject should be notified when a file is opened on him or a report is made on him. An Oklahoma statute, for example, requires that a copy of the report he submitted to the report subject and also requires a request asking him for a statement of his assets and liabilities.[60] But M.T. Pearson of the Association Credit Bureaus of Canada opposed such policies and states:

> ACB of C research into this matter indicates that either proposal would drive the cost of credit reporting up by at least 50 per cent. This could cripple virtually every Credit Bureau in Canada as a viable business enterprise.[61]

He claims this would cost the Credit Bureau of Montreal $190,000 per year, and the Credit Bureau of Edmonton $72,750 per year.[62] Perhaps a compromise can be considered in two provisions. One would be a prohibition against any requirement that the person receiving a report not inform the subject of the report that he has received it; in fact, the user should be encouraged to so inform him. An exception could be made

> where the data is not subject to access because of confidentiality. The other provision would be that a file must indicate all persons who have used the information for which subject access is available. The individual requesting access would observe this record. These suggestions are not submitted as firm proposals but only as a possible compromise that bears consideration.

The disciplinary wing of the regulatory agency, and the inspection staff of the agency, should be alert to detect failure to observe these duties and should be quick to give directives or warnings to give the system opportunity to comply before disciplinary action is taken.

ADMINISTRATIVE MACHINERY

The discussions of licensing, supervision of self-regulation by operators, and other regulations have made continual reference to a federal regulatory agency. Thus it is appropriate here to comment on the administrative machinery that would be required to implement the policy suggestions.

It is suggested that a centralized agency be set up with a qualified permanent staff. Costs could be borne by licensing fees, the public treasury, or possibly investment from a bonding fund furnished by system licensees. The licensing policy board and the disciplinary boards conducting hearings should be separated, with only the former maintaining any significant contact with other government agencies. This is suggested because the divisions should

not appear to be acting together as both prosecutor and judge, while government agencies themselves may employ the individuals whose conduct is in question. Perhaps the work space should be completely separated and the only linkage should be at the highest echelons of policy-making or responsibility. While the agency may report to an existing minister -- likely the minister responsible for Statistics Canada -- it should be independent from operating agencies of government and Statistics Canada so that there is less danger of agency personnel becoming hopelessly indoctrinated with the information-gathering views of these other agencies. The need for independence is stressed by many writers. Arthur R. Wright, noting pressures from carriers, shippers and consignees, and government on the Board of Transport Commissioners, stated that:

> In most cases the aims of these three interests are not only diverse but opposed to each other. In such a situation the independence of the Board is of utmost importance if the conflicting interests are to be resolved. It is this distinguishing characteristic of independence which is vital to the Board if it is to operate effectively and impartially.[63]

The agency here should encourage the information storage system industry, government, and civil liberties groups to make representations to it, but should aim for impartiality and independence for decision-making. The objective should always be a rational balance between policy and privacy needs.

Perhaps it would be appropriate to appoint the licensing body on a representative basis, with representatives from government, the information system operators, and the public. This group would be the senior policy-making group to establish licensing policy and develop an up-to-date code of conduct for the operators. In making policy, this body should promote representations from the interested groups to bring out points of view from various perspectives. One writer discussed this function and wrote:

> Rule making fulfills this need of licensing agencies to take hold of basic problems before they reach the stage of crisis or dispute. Not only is this procedure designed to develop policy in advance but, by allowing all interested parties an opportunity to be heard, it will invariably produce a wiser and fairer policy.[64]

This licensing wing could also supervise the permanent staff who would investigate complaints, issue licenses in non-contentious cases, perform audits or other procedures designed to assist enforcement of the policies, and keep informed of new developments. Since this staff would conduct prosecutions or present cases against an applicant for license, it appears preferable to provide that any hearings required on licensing applications or discipline should be conducted by the licensing and disciplinary tribunals of the disciplinary wing which exercise no supervision over the permanent staff.

This policy-making and supervisory body should also aim for close liaison with the communications industry.[65] Representatives from the communications industry could be members of the policy body, and they should at least be consulted whenever questions involving communications links for information storage systems are at issue. The communications issues are especially involved for computerized systems. Care should be taken, however, to avoid control of the communications industry by the data storage industry since, as Grenier states, "Any regulatory scheme which subjects a company to regulation directly by its customers must be viewed with a healthy skepticism."[66]

The body conducting hearings for controversial licensing applications or disciplinary actions could have a similar representative composition. It would be controlled by the licensing policy board only to the extent of general policy guidelines and, in the case of the government or occupational representatives (should there be no associations to appoint the latter), by tenured appointment. Lay members, who could possibly be lawyers experienced in the judicial process, could be appointed by the Governor-General in Council or other body outside the agency and could operate as chairmen for the three-man board hearings. They should bear responsibility for seeing that the public interest is not sacrificed to the interests of other groups and could insure that individuals are never denied their protective rights. Should a lawyer be the lay

representative, he could help to guard against technical violations of procedure which could invalidate decision if reviewed by a court.[67] The other representatives, particularly those from the occupation itself, should bring an expertise to the bodies which could be invaluable where sophisticated techniques are involved. These people should not sit on a case, however, when the operator or licensee being considered is an acquaintance or definite competitor. Three-man tribunals for discipline or licensing should be available in several centers in Canada on a full or part-time basis depending upon the demand for hearings. Appeal rights would be as discussed above under the Federal Court Act.

The permanent staff, supervised by the policy body, would exercise the responsibility for handling complaints in the first instance, and presumably would have discretion to dismiss frivolous and non-substantial complaints. Avoiding delay should be a major goal. The staff should consider it their duty to attempt to inform the public of this avenue of redress. Other responsibilities would be to conduct inspections, which could include examination of user audits, issue non-contentious licenses, prosecute or assist in the prosecution of serious offenders, and be responsible for storage of data from systems which have temporarily lost their licenses or ability to function. Staff members would have to be located throughout Canada wherever such functions had to be carried out. The staff should not be involved in promotion and development of new

systems, since this could place their impartiality for licensing and disciplinary matters in question.[68] However, the staff should keep in touch with new advances in order to be qualified to deal with technical matters and to advise the supervisory body of new developments with suggestions for policy changes to meet them.

STRICT LIABILITY

The project now turns from a consideration of privacy protection by regulation to protection by other legal means. The purpose of this section of the project is to consider the value of strict liability as a means of protecting the public from the effects of harmful disclosure of personal, confidential information by data banks. This calls for a consideration of the "fault - no fault" debate -- the advantages and disadvantages of strict liability -- and a brief examination of some current illustrations. This will lead to a decision in favour of strict liability, making it advisable to examine some specific issues in applying strict liability to the data bank context.

The policy of no liability without fault in tort law reached its zenith in the nineteenth century, and a noted author asserts that this was fostered by a desire to encourage the development of the new industry by enabling it to avoid responsibility if it conducted itself with reasonable respect for the safety of others.[69] A person was generally liable to compensate

an injured party only if the shift in loss was justified by his misconduct or, as in the leading case of Rylands v. Fletcher,[70] if the harm was caused by a dangerous substance brought onto the land and likely to cause harm if it escaped. At least two substantial changes have affected the system since then. The first of these is liability insurance which, by allowing the wrong-doer to shift most of the expense onto others, conflicts with the classical fault approach of having the wrongdoer pay. Large scale production has a similar effect since liability expenses may be passed from the wrongdoer onto his employer and from there onto the consumer in the form of higher prices. The other factor is the growing emphasis on the moral and social purpose of tort law, whereby the law serves to define one's duties to others and set the standards for their performance. Thus the modern "fault - no fault" debate, notably over automobile accident liability, takes place in a context where the traditional fault theory of the nineteenth century has been undermined.

Those who would remove the "fault" criterion for civil liability are met with various objections. One of these is the argument that fault liability is designed to punish, and thereby deter, intentional or negligent conduct which causes injury to others. The Privacy Act of British Columbia may reflect this approach by establishing tort liability for a person "wilfully and without a

claim of right" to violate another's right to privacy.[71] According to this view, it is only where such conduct exists that one can justify shifting the burden of loss onto the defendant. Thus Salmond wrote in an early edition of his text on torts that:

> Reason demands that a loss shall lie where it falls, unless some good purpose is to be served by changing its incidence; and in general the only purpose so served is that of punishment for wrongful intent or negligence. There is no more reason why I should insure other persons against the harmful results of my own activities, in the absence of any *mens rea* on my part, than why I should insure them against the inevitable accidents which result to them from the forces of nature independent of human actions altogether.[72]

Obviously such an approach could leave the innocent injured party without compensation. In this situation the ideal solution would be to have the costs shifted onto the public at large, or onto the recipients of an enterprise activity in which context the injury arose. This, as the modern author of the Salmond text points out, is what occurs with liability insurance and large scale production. Thus the "punitive" function of fault liability, and arguments based upon its preservation, may be countered with the compensation function whereby innocent parties are compensated by those best able to bear the expense.

A related argument is the assertion that the fault system is based upon popular support for the philosophy of individual responsibility. W. David Griffiths, Q.C., expressed this view clearly while dealing with auto accident compensation:

> Is it so offensive to one's special conscience to insist that the 20th century motorist be legally liable for his wrongs even though he may be insured against his wrongdoing? After all the fault system is based on the concept of individual responsibility which many regard as the backbone of a strong and healthy society. The removal of this concept in this field by allowing a person to benefit from his own fault could substantially weaken the entire concept of individual responsibility. It could develop a something-for-nothing attitude that is bound to carry over into every aspect of our life.[73]

It appears reasonable to accept the force of this argument in those areas where the concept of individual responsibility is workable -- where improper conduct can be observed and fault determined. This may not be the case in the larger data information systems where responsibility for an error in personal data or an unauthorized information disclosure may be difficult or impossible to determine. Where sources of information become untraceable, or where intricate computers subject to technical malfunction are employed, this may be especially true. The damage may be said to be a result of the operation of the data system as a whole -- what Professor Ehrenzweig could consider an unavoidable and insurable consequence of a lawful enterprise.[74] The best way to improve performance may be to provide technical and procedural protections for the system as a whole rather than to attempt to isolate individual responsibility and punish the wrongdoer. The proper legal approach would be one of "enterprise liability" whereby the loss must be met by the owners of the data system and passed on, as noted below, to those who benefit from it.

The question of costs may prompt another objection from advocates of "no liability without fault" since compensation for all persons suffering injury due to information system mistakes could raise the fear of crushing costs which could destroy the vitality of the private enterprises concerned. On the other hand, reduced litigation costs or wider distribution of cost are used by others to claim that the additional costs are not excessive.[75] In the case of commercial credit bureaus, the possibility of lower liability awards and the high level of accuracy claimed by the credit bureaus[76] could indicate that costs would not increase to a disastrous level with a strict liability scheme. The increased costs should ultimately be passed on to those who really benefit from credit bureau operations -- those who seek and those who grant credit.

There is another aspect to the costs factor also. As Griffiths put it:

> The proponents of the low cost plans often overlook the probability that any compensation plan based on liability without fault is going to develop in the public an unprecedented claims consciousness. The victim who at present is willing to bear marginal or trivial or doubtful losses will certainly be eager to file claims under the new system. With the increase in small claims there will be a proportionate increase in fraudulent claims. Compensation plans must in the interest of saving expenses, cut down investigation, particularly with respect to small claims and this reduced area of investigation will both encourage the filing of false claims and hinder the detection of frauds.[77]

Two points could be raised in reply. First of all, a plaintiff who is claiming against an information system should be required to prove the facts necessary to show the cause for complaint, and such essential prerequisites to liability as error in the data or consideration of the data by persons evaluating the data subject and making a negative decision would be difficult to manufacture fraudulently without the co-operation of several persons. Secondly, the lower litigation costs and greater likelihood of compensation for the plaintiff who need not prove fault will encourage persons with justifiable claims to come forward where they would not undertake the risk and expense before. In this way the true social cost of storing personal and confidential information in centralized systems will be more fully ascertainable, and more of these costs will be borne by those who benefit from the data storage.

A final argument to be dealt with is that based on the deterrent value of liability for fault -- the protection offered to the individual whose standard of conduct is maintained is an incentive to satisfy that standard. Two comments are relevant in reply. First of all, it may be doubted that the "fault" element in liability always operates as such an incentive in modern times. Fleming James Jr. wrote, after considering the effect of liability insurance on auto compensation, that:

> Since liability's burden is not borne by those at fault, it can scarcely operate directly as an effective deterrent against faulty conduct. To be sure those who must pay -- employers and insurers -- may use discipline, or higher premiums, or some other means, as incentives to safety on the part of motorists for whom they are responsible. And this may take the form of trying to forestall faulty conduct. But these pressures will be brought to bear whether the initial liability is based on fault or is imposed without it. Employers and insurers will try to reduce accidents in order to minimize the cost of their accident liability whatever its legal source.[78]

Secondly, it is probable that sufficient incentives for proper conduct exist outside the fault system so that its disappearance will have little effect. Such factors as procedural and technical criteria for license certification, administrative inspection, criminal sanctions, pressure from clientele, or higher insurance costs for operations with a poor liability record in the data storage field could be sufficient incentive for accuracy and protection of data.

The advantages of a "no fault" system have been partially indicated above, but it is worthwhile to summarize here some of the advantages of strict liability for harmful error or disclosure of confidential data. First of all, it provides compensation for all who become aware of a loss suffered by such error. Except for cases of misconduct or genuine verification by a data subject, for which legal exceptions are possible (see below), the individual has no control over the accuracy of the data stored

about him and should not be the one to suffer the loss even if he cannot demonstrate a fault by the operator. Furthermore, the plaintiff would find the expense and difficulty of proving fault removed from his shoulders, while the simplification of legal issues might lead to more settlements with less delay in compensation. The cost of this compensation should be largely reflected in the cost of data storage or provision to the client for, as Starn said in the case of commercial air carriers, "The airlines are merely a conduit, requiring the passengers to protect themselves from any risk of air travel by sharing the cost of that risk with their fellow travellers."[79]

A further advantage is that the imposition of strict liability could be sufficient penalty on the information system to make it unnecessary to use criminal sanctions for lesser violations of standards of conduct. This would reduce the burden of law enforcement agencies and courts, and would avoid the stigma of criminal liability for a person or enterprise whose departure from acceptable standards was only minor.

The above advantages need not undermine the regulation and control of the data banks since, as noted above, the removal of the focus on fault need not substantially reduce the incentive for the industry to maintain proper standards. Indeed, strict liability may even increase the benefits of precaution. As one author noted in an article favouring strict liability for harm caused by crop dusting:

> Moreover, imposing strict liability on crop dusters would encourage the taking of every possible safety precaution. For example, the likelihood of drift is substantially reduced by the use of helicopters, but at the present time the initial investment required for such equipment has deterred its use by most aerial applicators.[80]

By analogy, some of the more expensive encrypting, identification or other procedures may be come financially feasible for those who store confidential personal information under strict liability.

The above discussion indicates that, while some of the objections to liability without fault may be sound in situations where individual responsibility is a workable concept, there are specific areas where liability without fault may be more attractive. The illustrations below appear to indicate a trend consistent with this view.

While the authors of Winfield on Tort thought that liability for breach of a statutory duty requiring something to be done without qualification was automatic,[81] the courts have often held that where an activity is authorized by legislation liability will be found only if the defendant was negligent.[82] Breach of the statutory duty may be evidence of the negligence. Other statutes deal more specifically with civil liability. An early statute, The Fires Prevention (Metropolis) Act, 1774,[83] protected the person on whose premises a fire had "accidentally" begun from civil liability

for damage suffered thereby. A later statute, however, concerning fire may have reflected a growing desire to protect those who suffer from industrial progress. Previous decisions had held that statutory authorization of railroads protected them from liability for fires caused by sparks and cinders if the railroad had taken available precautions,[84] but by The Railway Fires Act, 1905, as amended in 1923, Parliament provided that where damage thus occurred to agricultural land or crops ". . . the fact that the engine was used under statutory powers shall not affect liability in an action for damage."[85] An interesting feature was that by s. 1(3) the Act only applied where the claim did not exceed two hundred pounds. A more modern illustration is provided by both Canadian and United Kingdom imposition of absolute liability on operators of industrial nuclear installations for damage caused by escape of radioactive substances. The Canadian Nuclear Liability Act imposes the liability without proof of fault or negligence and requires that the operator be insured for seventy-five million dollars.[86] Furthermore, several of the provinces in Canada have now moved to no fault liability for automobile accident compensation while, as a look at the bibliography indicates, there are active suggestions for strict liability for air carriers and crop dusters as well.

At common law, strict or very severe civil liability applies to ultra-hazardous activities or "things dangerous in themselves."[87] Laidlaw, J.A., stated in Dokuchia v. Domansch[88] that the rule in Rylands v. Fletcher "is not confined to liability of landowners to each other but makes the owner of the dangerous thing liable 'for any mischief thereby occasioned.'" In the case of civil liability for fire-arms, John de P. Wright asserts that, while the defendant may succeed if he satisfies the onus of establishing the absence of both intention and negligence, the duty of care is "so high that it borders upon strict liability."[89] In the processing and manufacturing fields, the United States appears to be moving toward strict liability where injury results from improper foods or products.[90] In Canada and Great Britain, however, strict liability to consumers has not been fully developed because the remedies in contract and negligence have provided strong protection for the plaintiff.[91] In the area of defamation, which has some similarity to potential liability for harmful disclosure of confidential data, the defendant may be liable even though he was unaware of the defamatory implications of the statement.[92] The plaintiff in some Canadian provinces does not have to prove damages to succeed in defamation cases,[93] while in others certain types of slander are recognized to be actionable without proof of damage.[94] Thus it appears likely that, with the growing complexity and potential for harm of large scale data storage systems, legislation imposing strict liability for harmful disclosure of confidential information would be consistent with the trend illustrated in statutory and judge-made law.

If strict liability is to be established for harmful disclosure of personal, confidential information, important issues are raised. The first of these is the need to decide just when the liability applies -- what situation must a plaintiff show before he can succeed. It seems reasonable to the author that liability should not lie unless: a) the information came from an information storage system (as defined); b) the information concerned an identifiable person; and either c) the information was confidential or sensitive (as defined) and no proper authorization was obtained from the subject for its release, or d) the information was both i) erroneous and ii) distributed to someone who had a decision concerning that person which was unfavourable to him and for which, on an objective basis, the information could have affected the decision. It is hoped that the plaintiff here faces a burden of proof which is substantial enough to protect operators from frivolous claims but is, with the need to prove fault removed, light enough to enable just claims to succeed.

Further provisions appear necessary to support the effectiveness of such a system. The operator, as owner of the system, should be required to show proof of financial responsibility before his data bank can obtain the license necessary to operate (as discussed above). The system should also be prohibited from obtaining a release from indemnity from any person except in the case of settle-

ment of a claim. Vicarious liability rendering the employer liable for the defaults of any employees would be implied in the strict liability, but it may be only proper to allow him to obtain indemnity from any employee found responsible by intention or recklessness for a default, particularly if damage awards are not expected to be excessively high.

Another issue concerns the rights of the systems owners to some defences against unjustified claims. The above discussion indicates that truth is a defense where the information is not confidential, while full consent to disclosure is a defense where it is confidential. Another defense should be fault or negligence by the plaintiff. Since many persons have carelessly or even wilfully given incorrect information when completing forms or being interviewed, the information storage system can be expected to contain many bits of erroneous information for which the individual who is to blame should be the one responsible. Another defense for medical records only is that of emergency where the information was believed on reasonable grounds to be necessary for medical aid. A final defense would be verification, but this would have to be carefully defined. Where an individual has requested or has been given access to his information file, has examined it <u>fully</u>, and has accepted its accuracy, it would appear unjust to saddle the system with liability for error in the file where the information in question was in the file at the time of verification.

The burden of proof in litigation must also be defined. One device which is often used to create a situation similar to strict liability in cases where the instrumentality causing damage is exclusively under the defendant's control, and is likely to cause damage only if the defendant is negligent, is the maxim res ipsa loquitur -- "the thing speaks for itself." The plaintiff must prove that the damage occurred in such a context, whereupon the defendant must prove that he was not negligent. Nevertheless, this device does not always have the same effect as strict liability because the plaintiff will still be required to prove fault if the defendant can show that he took all reasonable precautions. Since the plaintiff likely has no knowledge of what happened in the defendant's premises, he will be burdened with the whole loss even though he had no control over the instrumentality which produced it. The better course would be to require the plaintiff to prove the facts required to ground a claim, whereupon the defendant would be liable unless he could prove that one of the defences noted above was applicable.

A final issue to be considered is the very important question of damages. In the past, although damages could be awarded irrespective of any actual or probable financial loss,[95] the prospect of low damage awards for a plaintiff even after he had managed to prove fault likely acted as a deterrent to the bringing of actions against credit bureaus or similar bodies. Furthermore, it is difficult

in some cases to determine the actual loss which the plaintiff has suffered in the case of a harmful disclosure of personal information. For these reasons, it is suggested that breach of duty in this area be actionable without proof of damage. This is the case in many of the provincial defamation statutes and in the two provinces where privacy acts have been passed.[96] It is submitted that legislation should have a section reflecting an approach similar to that of section 4(2) of The Privacy Act in Manitoba, which reads:

> 4(2). In awarding damages in an action for a violation of privacy of a person, the court shall have regard to all the circumstances of the case including
>
> (a) the nature, incidence and occasion of the act, conduct or publication constituting the violation of privacy of that person;
>
> (b) the effect of the violation of privacy on the health, welfare, social, business or financial position of that person or his family;
>
> (c) any relationship, whether domestic or otherwise between the parties to the action;
>
> (d) any distress, annoyance or embarrassment suffered by that person or his family arising from the violation of privacy; and
>
> (e) the conduct of that person and the defendant, both before and after the commission of the violation of privacy, including any apology or offer of amends made by the defendant.

While item c) may not be relevant, factors such as the relationship between the recipient of the information and the subject, the extent of publication of the information, and the degree of sensitivity of

it would appear material. The making of a reasonable mistake or the circulation of an apology and correction should be relevant in mitigation of damages, much as they are in cases of defamation. In cases where malice or serious neglect are involved, the courts may consider punitive damages as a useful instrument, especially since Canadian courts are not as restricted in their use as the British courts are.[97] As Professor Fridman asserts:

> . . . awards of punitive damages may be regarded as fulfilling the purpose and function of the law of torts, in that such awards may well indicate the displeasure of the law that its standards are not being fulfilled and may assist the law in the imposition of those standards.[98]

Thus, while there are some sound objections to the wholesale use of strict liability, there are instances where it can serve as a useful means of protecting the public and promoting the maintenance of proper standards of conduct. It is hoped that, with the addition of some of the features described above, strict liability may serve to uphold public interests in the operation of large-scale information storage systems.

OTHER MATTERS OF CIVIL LAW

The regulatory provisions and imposition of strict liability need not imply the removal of other civil remedies which have been available in the past. While actions like those for defamation, loss of privacy, or negligence may be less attractive

for individuals who can claim under the strict liability provisions, they could remain useful for cases involving data of a corporation or non-individualized data belonging to someone other than the body storing the data. Accordingly, it is beneficial to make brief mention of a few other concepts of civil law which may be of value for privacy protection.

Those who have commercial or statistical data in an information storage system belonging to someone else could consider contract as a means to protect themselves in the event of an undesired disclosure of data. As Charles P. Lickson comments, "When privacy of data communications has taken on the tenor of a contractual term, a definitive amount of protection is assured. To deny protection would then constitute a breach of contract as well as a failure to supply the requested services."[99] He notes that a contract could set out a general duty of protection, required technical safeguards, or even appropriate damages for breach of the contract. An interesting aspect of this was raised by Grenier who claimed that an individual employee who has suffered a harmful disclosure of personal information from his employer's files stored by the system may seek recovery from the storage company as a third party beneficiary of the contract.[100] There appears to be no need for specific interference by the federal government in the contract area, except of course to prohibit terms which require an information user not to disclose that he has received information on a person from a storage system which merges data on individuals from various sources.

The contract method above and other rights at civil law involve the need for a proprietary concept for the data. Professor Miller does not believe that property concepts are very useful for privacy protection since they are intended to deal with legal title and exploitation rights rather than protection against disclosure, and are too inflexible to deal with new developments.[101] However, some concept of identifiable interest would seem necessary to deal with situations of data storage for a customer by a storage system. While property concepts may be easy to adapt to situations involving physical files in manilla folders, they may be less capable of dealing with computer storage. Professor Lederman, however, believes that "Intelligent use of analogy and imaginative invention of new types of rights, where necessary, should enable us to deal properly with the 'property' problems of electronic data processing."[102]

The development of proprietary concepts could support other remedies or protections at civil law. One interesting application is that of the trust which is used by the United Planning Organization in the United States and involves the designation of trustees for the data.[103] Although Professor Miller raises problems with this method in areas of enforceability, rights of parties outside the trust, uniformity, and creation ex parte by the party controlling the data base,[104] it may be a useful arrangement in some cases. Another right dependent upon proprietary rights would be an action in trespass, and this could be appropriate for cases where one party interferes with the data of another.[105]

CRIMINAL LAW

A role should remain for the criminal law as a means to protect privacy from abuse of data accumulation. However, the licensing scheme for systems and supervisory regulation of system operators, with the penalties resulting from unacceptable conduct as outlined above, coupled with the strict liability for improper disclosure of information, should provide sufficient sanctions to discourage unsatisfactory actions in the majority of cases. Criminal law could then be used only for the most serious acts of wilful invasion of privacy. One example of such conduct could be an unauthorized, intentional intrusion into the data storage system by physical or other means with the purpose of observing, acquiring, altering or destroying data to which the intruder has no colour of right. Another example could be wire-tapping or other interception of communications of sensitive or confidential data. The use of general phrases like "other means" or "other interception" is intended to avoid the situation where a novel means of interfering with data becomes immune from criminal sanction due to obsolete legislation; the focus is upon acts of any sort intended to obtain or interfere with data to which the actor has no right, regardless of whether it is being stored or communicated at the time.[106] A final example for which criminal sanction is appropriate would be the theft or counterfeiting of authorization indicia, whether it be in the form of a wafer, card, or code.

In the broader sphere, Edward F. Ryan puts forward the idea of creating a crime of invasion of privacy, to include institutional, corporate and trade union privacy as well as that of individuals.[107] He goes on to add the precaution that, "The crime of invasion of privacy should be limited to the most serious manifestations of spying, with the law of tort invoked by private individuals being the agency through which the remaining majority of abuses is controlled."[108] Looking only at the information storage issue, perhaps this idea should not be adopted unless experience shows that the new regulatory and civil controls provide insufficient discouragement for privacy violation.

CONCLUSION

The purpose of this project has been to consider means for the federal government to guard against excessive erosion of privacy by information storage systems containing personal data. Concern has been developed by the technological progress which has enormously increased data manipulation and storage capacity, but has also revealed a need to act now to insure that citizens of Canada can reap the benefits and minimize the detriments of such developments. Hopefully some of the ideas and schemes presented here can provide a means to that end. Although they have been presented in the advocative style, it is hoped that their potential drawbacks have been sufficiently set out so that we will not fail to reject or alter them should this be the wiser course.

FOOTNOTES

1. Kenneth Cheng, Ph.D., "Privacy and Data Bank." Paper presented at the "Computers and the Law Conference," Queen's University, Kingston, Ontario, June 1-3, 1968, page 5.

2. John de J. Pemberton, Jr., "On the Dangers, Legal Aspects, and Remedies," in "Symposium: Computers, Data Banks and Individual Privacy" (1968), 53 Minnesota Law Review 211, 223.

3. Jerry M. Rosenberg, The Death of Privacy. New York: Random House, 1969, p. 81. Chapter III contains an illuminating discussion of current data storage in the private sector.

4. Arthur R. Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society" (1969), 67 Michigan Law Review 1089, 1103.

5. Edward J. Grenier, Jr., "Computers and Privacy: A Proposal for Self-Regulation" (1970), Duke Law Journal 495, 505.

6. Miller, op. cit., p. 1111.

7. Canada Grain Act, R.S.C. 1970, c. G-16, ss. 79 and 89.

8. Stevedoring Reference (1955) S.C.R. s. 29; Commission du Salaire Minimum v. Bell Telephone (1967), 59 D.L.R. (2d) 145 (S.C.C.)

9. Hugh Lawford, A.J. de Grandpre, W.R. Lederman, J.S. Grafstein, "The International Legal Problems of Computer Communications: Automation of the Transnational Information Flow" (1970), 20 University of Toronto Law Journal 337, 345.

10. Kenneth Cheng, Ph.D., "Privacy and Data Bank" (1969), 17 Chitty's Law Journal, 90, 92.

11. See Albert Mindlin, "Confidentiality and Local Information Systems" (1968), 28 Public Administration Review 509.

12. Grenier, op. cit.

13. Extract in Senate Subcommittee Hearings at p. 298 from "Legal Safeguards to Insure Privacy in a Computer Society" (1967), 10 Communications of the A.C.M., No. 9.

14. Miller, op. cit., p. 1188.

15. E.g. W.R. Lederman in Lawford, et al., op. cit., pp. 348-349; Rosenberg, op. cit., p. 183.

16. Ian Rodger, "Computers: Privacy and Freedom of Information," Report on Conference at Queen's University, 1968, pp. 45-48.

17. Mindlin, op. cit., p. 516.

18. Kenneth L. Karst, "'The Files': Legal Controls over the Accuracy and Accessibility of Stored Personal Data" (1966), 31 Law and Contemporary Problems 342, 343, 344.

19. Miller, op. cit., p. 1187.

20. Comment, "Computer Retrieval of the Law: A Challenge to the Concept of Unauthorized Practice?" (1968), 11 University of Pennsylvania Law Review, 1261, 1282.

21. John W. MacDonald, "The Need for Standards in the Selection of Licensees" (1964), 17 The Administrative Law Review 61; Robert A. Hyerle, "License Revocation: Uncertainty and Due Process" (1963-64), 15 The Hastings Law Journal 339.

22. Ontario, Royal Commission Inquiry into Civil Rights, Volume 3, Report No. 1, page 1190. The Report is hereinafter referred to as the McRuer Commission Report.

23. Miller, op. cit., p. 1209.

24. Alan F. Westin, "Legal Safeguards to Insure Privacy in a Computer Society" (1967), 10 Communications of the A.C.M. 533, 536.

25. The audit procedure is given favourable comment in Roy N. Freed, "A Legal Structure for a National Medical Data Center" (1969), 49 Boston University Law Review, 79, 93.

26. See Grenier, op. cit.

27. John T. Tansey and F. Lee Ruck, "Conditional Broadcasting Licenses; Defining the Legal Perimeters" (1965), 33 George Washington Law Review 764; James C. Robertson, "Administrative Regulation by Conditions in Certificates of Public Convenience and Necessity" (1968), 21 Stanford Law Review, 188.

28. Canada Grain Act, R.S.C. 1970, c. G-16, s. 79(3).

29. Freed, op. cit., p. 90.

30. Ibid., p. 92.

31. See Note, "Entrance and Disciplinary Requirements for Occupational Licensees in California" (1962), 14 Stanford Law Review 533, 535, and William C. Keck, "Occupational Licensing: An Argument for Asserting State Control" (1968), 44 Notre Dame Lawyer 104, 109.

32. Cory Brundage, "Disciplinary Enforcement Problems and Recommendations: An Indiana Survey" (1970), 46 Indiana Law Journal, 134.

33. Philip J. Hoblin, Jr., "A Stock Broker's Implied Liability to its Customer for Violation of a Rule of a Registered Stock Exchange" (1970), 39 Fordham Law Review, 253, 269.

34. Morris J. Dean, "The Opportunity to be Heard in the Professional Licensing Process in Pennsylvania," (1962-63), 67 Dickinson Law Review, 31, 40.

35. The Administrative Procedure Act, 5 U.S.C. #1008 (b), sec. 9(b) (1946).

36. Note, "Procedural Safeguards for Licensees: Section 9(b) of the APA" (1961), 75 Harvard Law Review 383, 388.

37. For example, see John J. Marotta, "Agency Access to Credit Bureau Files: Federal Invasion of Privacy?" (1970), 12 Boston College Industrial and Commercial Law Review 110, 125, and his proposal for an independent federal agency, the Data Processing and Management Office.

38. Mindlin, op. cit., p. 513.

39. Marotta, op. cit.

40. Miller, op. cit., p. 1235.

41. Ibid., p. 1219.

42. F.A.R. Bennion, Professional Ethics. London: Charles Knight & Co. Ltd., 1969, p. 202.

43. Great Britain, "Computers and Personal Records: Motion for papers read, debated and withdrawn," December 3, 1969, 306 H.L. Debates 103.

44. Jack R. Frymier, "Professionalism in Context" (1965), 25 Ohio State Law Journal 53, 64.

45. Supra, footnote 31.

46. McRuer Commission Report, Vol. 3, report no. 1, sections 2 and 4.

47. Brundage, op. cit.

48. Alan F. Westin, "Science, Privacy and Freedom: Issues and Proposals for the 1970's" (1966), 66 Columbia Law Review 1003; 1205, at p. 1219.

49. Miller, op. cit., p. 1153.

50. Harry N. MacLean, "Brokers' Liability for Violation of Exchange and NASD Rules" (1970), 47 Denver Law Journal 63, 72.

51. Ibid., p. 75.

52. H.W. Arthurs, "Authority, Accountability and Democracy in the Government of the Ontario Legal Profession" (1971), 49 Canadian Bar Review 1, 8.

53. For an interesting statement of proposed qualifications for successful self-regulation see the Canadian Committee on Mutual Funds and Investment Contracts Report, CCH Securities Law Reporter, Volume 2, 70-002, p. 12, 502, recommendation (1).

54. Miller, op. cit., p. 1221.

55. Quoted in Frymier, op. cit., p. 57.

56. Barry I. London, Geoffrey C. Lord, and Paul M. Schaeffer, "Admission to the Pennsylvania Bar: The Need for Sweeping Change" (1970), 118 University of Pennsylvania Law Review 945.

57. Robert W. Hallock, "Civil Remedies and Stock Exchange Rules -- An Emerging Concept of Implied Liability" (1969), University of Illinois Law Forum 561.

58. "Entrance and Disciplinary Requirements for Occupational Licensees in California," op. cit., p. 549.

59. McRuer Commission Report, Vol. 3, Report No. 1, p. 1190.

60. Oklahoma Statutes Annotated, Title 24, c. 4, Nos. 81 and 82.

61. The Associated Credit Bureaus of Canada, M.T. Pearson, General Manager, "Data Bank for Credit Bureaus," Position Paper for Conference on Computers: Privacy and Freedom of Information, Queen's University, May 21-24, 1970, p. 12.

62. Ibid., p. 13.

63. Arthur R. Wright, "An Examination of the Role of The Board of Transport Commissioners for Canada as a Regulatory Tribunal" (1963), 6 Canadian Public Administration 349, 363.

64. Dean, op. cit., p. 52.

65. This need for communications liaison is stressed by Grenier, op. cit.

66. Ibid.,pp. 510-511.

67. Legal counsel for licensing boards are advocated in Robert C. Derbyshire, M.D., Medical Licensure and Discipline in the United States. Baltimore: The Hopkins Press, 1969, p. 17.

68. See David Cavers, "Administrative Decisionmaking in Nuclear Facilities Licensing" (1962), 110 University of Pennsylvania Law Review 330, 331.

69. John G. Fleming, The Law of Torts, 3rd ed. Australia: The Law Book Company of Australia Pty. Ltd., 1965, p. 289.

70. Rylands v. Fletcher (1868), L.R. 3 H.L. 330.

71. Privacy Act, Stats. B.C. 1968, c. 39, s. 2(1).

72. Quoted in R.F.V. Heuston, Salmond on the Law of Torts, 15th ed. London: Sweet and Maxwell, 1969, p. 26.

73. W. David Griffiths, Q.C., "Don't abolish tort law in auto accident compensation" (1969), 12 Canadian Bar Journal, 187, 190.

74. Albert A. Ehrenzweig, Negligence Without Fault: Trends toward an Enterprise Liability for Insurable Loss. Berkeley: University of California, 1951.

75. See Peter Starn, "Domestic Commercial Aircraft Tort Litigation: A Proposal for Absolute Liability of the Carriers" (1971), 23 Stanford Law Review 569, 582-590 for costs in commercial air travel.

76. See the Paper by M.T. Pearson of the Associated Credit Bureaus of Canada, supra, footnote 58. Note Table I.

77. Griffiths, op. cit., p. 195.

78. Fleming James, Jr., "An Evaluation of the Fault Concept" (1965), 32 Tennessee Law Review 394, 399.

79. Starn, op cit., p. 581.

80. George C. Chapman, "Crop Dusting -- Scope of Liability and a Need for Reform in the Texas Law" (1962), 40 Texas Law Review 527, 536.

81. J.A. Jolowicz, T. Ellis Lewis, Winfield on Tort, 8th ed. London: Sweet and Maxwell, 1967, p. 18.

82. Allen M. Linden, "Strict Liability, Nuisance and Legislative Authorization" (1966), 4 Osgoode Hall Law Journal 196.

83. 14 Geo. 3, c. 78, s. 86, reprinted in Halsbury's Statutes of England, 3rd. ed., Vol. 17.

84. Vaughn v. Taff Vale Railway (1866), 29 L.J. Exch. 247.

85. 5 Edw. 7, c. 11, s. 1(1), reprinted in Halsbury's Statutes of England, 2nd. ed., Vol. 19.

86. Nuclear Liability Act, Stats. Can. 1970, c. 29 (1st Supp.), s. 4 and s. 15.

87. Lord Dunedin in Dominion Natural Gas Company Limited v. Collins, Perkins and Others (1909) A.C. 640, 646 (P.C., appeal from Ontario).

88. Dokuchia v. Domansch (1945), O.R. 141, 146 (C.A.).

89. John de P. Wright, "Civil Liability for Fire-Arms" (1968), 11 Canadian Bar Journal 247, 248.

90. H.P. McLaughlin and M.S. Shannon, "'Caveat Factor': Strict Liability and the Manufacturer" (1964-66), 2 University of British Columbia Law Review 502, 508.

91. Ibid., p. 512.

92. E. Hulton & Co. v Jones (1910) A.C. 20.

93. The Defamation Act, R.S.M. 1970, c. D20, s. 3. Similar provisions are in the statutes of Alberta, New Brunswick and Prince Edward Island.

94. E.g., The Libel and Slander Act, R.S.O. 1960, c.211, ss. 17-19.

95. Sakowski v. Rusiecki (1960), 67 Man. R. 256, 258 (Q.B.).

96. The Privacy Act, Stats. Man. 1970, c. 74, s. 2(2) and the Privacy Act, Stats. B.C. 1968, c. 39, s. 2(1).

97. See G.H.L. Fridman, "Punitive Damages in Tort" (1970), 48 The Canadian Bar Review 373.

98. Ibid., p. 404.

99. Charles P. Lickson, "Protection of the Privacy of Data Communications by Contract: Another Case Study on The Impact of Computer Technology on the Law" (1968), 23 The Business Lawyer 971, 980-81.

100. Grenier, op. cit., p. 499.

101. Miller, op. cit., p. 1224-25.

102. Supra, footnote 9, p. 348.

103. This arrangement was discussed by Wiley Branton, Executive Director of the U.P.O., at the Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate, February 6, 1968.

104. Miller, op. cit., p. 1226-1228.

105. Society of Conservative Lawyers, Computers and Freedom. Conservative Research Department, December 1968, p. 8.

106. Some of these problems have existed with previous legislation -- see Grenier, op. cit. for comment on American action in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

107. Edward F. Ryan, "Protection of Privacy -- A Call for Federal Action" (1969), 17 Chitty's Law Journal 218, 219.

108. Ibid.

BIBLIOGRAPHY

Arthurs, H.V. "Authority, Accountability, and Democracy in the Government of the Ontario Legal Profession." (1971), 49 Canadian Bar Review 1.

Associated Credit Bureaus of Canada, The. M.T. Pearson, General Manager, "Data Banks for Credit Bureaus." Position Paper for Conference on Computers: Privacy and Freedom of Information, Queen's University, May 21-24, 1970.

Baugher, William Edward. "Interagency Information Sharing: A Legal Vacuum." (1969), 9 Santa Clara Lawyer 301.

Bennion, F.A.R. Professional Ethics. London: Charles Knight & Co., 1969.

Brundage, Cory. "Disciplinary Enforcement Problems and Recommendations: An Indiana Survey" (1970), 46 Indiana Law Journal 134.

Canadian Committee on Mutual Funds and Investment Contracts, Report. Released December 9, 1969. Canadian Securities Law Reporter, Volume 2: C.C.H. Canada Ltd., 70-002, #12,501.

Cavers, David F. "Administrative Decisionmaking in Nuclear Facilities Licensing." (1962), 110 University of Pennsylvania Law Review 330.

Chapman, George C. "Crop Dusting -- Scope of Liability and a Need for Reform in the Texas Law." (1962), 40 Texas Law Review 527.

Cheng, Kenneth. "Privacy and Data Bank." (1969), 17 Chitty's Law Journal 90.

Cheng, Kenneth. "Privacy and Data Bank." Paper Presented at the "Computers and the Law Conference," Queen's University, June 1-3, 1968.

Comment. "Computer Retrieval of the Law: A Challenge to the Concept of Unauthorized Practice?" (1968), 116 University of Pennsylvania Law Review 1261.

Davison, Calvin; Babcock, Stephen L.; Leshy, John D. "Computers and Federal Regulation." (1969), 21 The Administrative Law Review 287.

Dean, Morris J. "The Opportunity to be Heard in the Professional Licensing Process in Pennsylvania." (1962-63), 67 Dickinson Law Review 31.

Derbyshire, Robert C., M.D. Medical Licensure and Discipline in the United States. Baltimore: The Johns Hopkins Press, 1969.

Ehrenzweig, Albert A. Negligence Without Fault: Trends towards an Enterprise Liability for Insurable Loss. Berkeley: University of California, 1951.

Fleming, John G. The Law of Torts. 3rd ed. Australia: The Law Book of Australasia Pty. Ltd., 1965.

Freed, Roy N. "A Legal Structure for a National Medical Data Center" (1969), 49 Boston University Law Review 79.

Fridman, G.H.L. "Punitive Damages in Tort." (1970), 48 Canadian Bar Review 373.

Frymier, Jack R. "Professionalism in Context." (1965), 26 Ohio State Law Journal 53.

Gibson, R. Dale; Sharp, John M. Privacy and Commercial Reporting Agencies. Winnipeg: Legal Research Institute of the University of Manitoba, 1968.

Great Britain. "Computers and Personal Records: Motion for papers read, debated and withdrawn." 306 House of Lords Debates, No. 17, page 103 (December 3, 1969).

Green, John, Q.C. "A Fish Out of Water; Classical Fault on the Highway." (1970), 35 Saskatchewan Law Review 2.

Grenier, Edward J., Jr. "Computers and Privacy: A Proposal for Self-Regulation." (1970), Duke Law Journal 495.

Griffiths, W. David, Q.C. "Don't abolish tort law in auto accident compensation." (1969), 12 Canadian Bar Journal 187.

Hallock, Robert W. "Civil Remedies and Stock Exchange Rules -- An Emerging Concept of Implied Liability." (1969), University of Illinois Law Forum 551.

Harring, Janet S. "Liability Without Fault: Logic and Potential of a Developing Concept." (1970), Wisconsin Law Review 1201.

Heuston, R.F.V. Salmond on the Law of Torts, 15th ed. London: Sweet & Maxwell, 1969.

Hablin, Philip J., Jr. "A Stock Broker's Implied Liability to its Customer for Violation of a Rule of a Registered Stock Exchange." (1970), 39 Fordham Law Review 253.

Hyerle, Robert A. "License Revocation: Uncertainty and Due Process." (1963-64), 15 The Hastings Law Journal 339.

International Commission of Jurists. "Nordic Conference on the Right to Privacy." (1967), Bulletin of the International Commission of Jurists, No. 31.

"Invasion of Privacy: Use and Abuse of Mail Covers." (1968), 4 Columbia Journal of Law and Social Problems 165.

James, Fleming, Jr. "An Evaluation of the Fault Concept." (1965), 32 Tennessee Law Review 394.

Jolowicz, J.A.; Lewis, T. Ellis. Winfield on Tort. 8th ed. London: Sweet & Maxwell, 1967.

Karst, Kenneth L. "'The Files': Legal Controls over the Accuracy and Accessibility of Stored Personal Data." (1966), 31 Law and Contemporary Problems 342.

Keck, William C. "Occupational Licensing: An Argument for Asserting State Control." (1968), 44 Notre Dame Lawyer 104.

Lawford, Hugh; de Grandpre, A.J.; Lederman, W.R.; Grafstein, J.S. "International Legal Problems of Computer Communications: Automation of the Transnational Information Flow." (1970), 20 University of Toronto Law Journal 337.

"Liability Without Fault." (1965), 13 Chitty's Law Journal 163; 191.

Lickson, Charles P. "Protection of the Privacy of Data Communications by Contract: Another Case Study on the Impact of Computer Technology on the Law." (1968), 23 The Business Lawyer 971.

Linden, Allen M. "Strict Liability, Nuisance and Legislative Authorization." (1966), 4 Osgoode Hall Law Journal 196.

London, Barry J.; Lord, Geoffrey C.; Schaeffer, Paul M. "Admission to the Pennsylvania Bar: The Need for Sweeping Change." (1970), 118 University of Pennsylvania Law Review 945.

MacDonald, John W. "The Need for Standards in the Selection of Licensees." (1964), 17 The Administrative Law Review 61.

MacLean, Harry N. "Brokers' Liability for Violation of Exchange and NASD Rules." (1970), 47 Denver Law Journal 63.

Marotta, John J. "Agency Access to Credit Bureau Files: Federal Invasion of Privacy?" (1970), 12 Boston College Industrial and Commercial Law Review 110.

McGrady, Leo. "Compensation Scheme or Tort Liability." (1966), 2 Manitoba Law Journal 49.

McKay, Robert B. "An Administrative Code of Ethics: Principles and Implementation." (1961), 47 American Bar Association Journal 890.

McLaughlin, M.P.; Shannon, M.S. "'Caveat Factor': Strict Liability and the Manufacturer." (1964-66), 2 University of British Columbia Law Review 502.

Meldman, Jeffrey A. "Centralized Information Systems and the Legal Right to Privacy." (1969), 52 Marquette Law Review 335.

Merritt, Roger J. "Banks and Banking: Florida Adopts a Duty of Secrecy." (1970), 22 University of Florida Law Review 482.

Miller, Arthur R. "Personal Privacy in the Computer Age -- The Challenge of a New Technology in an Information-Oriented Society." (1969), 67 Michigan Law Review 1089.

Miller, J. Gareth. "The Disciplinary Jurisdiction of Professional Tribunals." (1962), 25 Modern Law Review 531.

Mindlin, Albert. "Confidentiality and Local Information Systems." (1968), 29 Public Administration Review 509.

Nader, Ralph. "The Dossier Invades the Home." Saturday Review, April 17, 1971, page 18.

Note. "Credit Investigations and the Right to Privacy: Quest for a Remedy." (1969), 57 The Georgetown Law Journal 509.

Note. "Entrance and Disciplinary Requirements for Occupations Licenses in California." (1962), 14 Stanford Law Review 533.

Note. "Procedural Safeguards for Licensees: Section 9(b) of the APA." (1961), 75 Harvard Law Review 383.

Ontario. Royal Commission Inquiry into Civil Rights. Report #1, Volume 3, sections 2 and 4.

"Privacy and Efficient Government: Proposals for a National Data Center." (1968), 82 Harvard Law Review 400.

Roberton, James C. "Administrative Regulation by Conditions in Certificates of Public Convenience and Necessity." (1968), 21 Stanford Law Review 188.

Rodger, Ian. "Computers: Privacy & Freedom of Information." Report on Conference at Queen's University, 1970.

Rosenberg, Jerry M. The Death of Privacy. New York: Random House, 1969.

Ryan, Edward F. "Protection of Privacy -- A Call for Federal Action." (1969), 17 Chitty's Law Journal 218.

Sharp, John M. Credit Reporting and Privacy. Toronto: Butterworths, 1970.

Silver, Martin. "A Survey of Views on Motor Vehicle Accident Compensation and the Concept of Fault." (1963), 2 Osgoode Hall Law Journal 452.

Society of Conservative Lawyers. Computers and Freedom. Conservative Research Department, December 1968.

Starn, Peter. "Domestic Commercial Aircraft Tort Litigation: A Proposal for Absolute Liability of the Carriers." (1971), 23 Stanford Law Review 569.

"Symposium: Computers, Data Banks, and Individual Privacy." (1968), 53 Minnesota Law Review 211.

Tansey, John T.; Ruck F. Lee. "Conditional Broadcasting Licenses -- Defining the Legal Perimeters." (1965), 33 George Washington Law Review 764.

United Nations Economic and Social Council, Report of the Secretary-General. "The Application of Computer Technology for Development." E/4800. May 20, 1970.

United States. Hearings Before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate. "Computer Privacy." February 6, 1968.

Vollmer, Howard M.; Mills, Donald L. Professionalization. Englewood Cliffs, New Jersey: Prentice-Hall, 1966.

Westin, Alan F. "Science, Privacy, and Freedom: Issues and Proposals for the 1970's." (1966), 66 Columbia Law Review 1003; 1205.

Westin, Alan F. "Special Report -- Legal Safeguards to Insure Privacy in a Computer Society." (1967), 10 Communications of the ACM 533.

Wright, Arthur R. "An Examination of the Role of The Board of Transport Commissioners for Canada as a Regulatory Tribunal." 6 Canadian Public Administration 349.

Wright, John de P. "Civil Liability for Fire-Arms." (1968), 11 Canadian Bar Journal 247.

STUDIES COMMISSIONED BY THE TASK FORCE

The Nature of Privacy - D.N. Weisstub and C.C. Gotlieb.

Personal Records: Procedures, Practices, and Problems - J.M. Carroll and J. Baudot, Carol Kirsh, J.I. Williams.

Electronic Banking Systems and Their Effects on Privacy - H.S. Gellman.

Technological Review of Computer/Communications.[1]

Systems Capacity for Data Security - C.C. Gotlieb and J.N.P. Hume.

Statistical Data Banks and Their Effects on Privacy - H.S. Gellman.

Legal Protection of Privacy - J.S. Williams.

Vie Privée et Ordinateur Dans le Droit de la Province du Québec - J. Boucher.

Regulation of Federal Data Banks - K. Katz.

Regulatory Models - J.M. Sharp.

Ordinateur et Vie Privée: Techniques et Contrôle - C. Fabien.

The Theory and Practice of Self-Regulation - S.J. Usprich.

Privacy, Computer Data Banks, Communications and the Constitution - F.J.E. Jordan.

International Factors - C. Dalfen.

[1] A joint Study by the Privacy and Computers Task Force and the Canadian Computer/Communications Task Force, to be published by the latter.