Dalhousie Law Journal

Volume 11 | Issue 2 Article 5

3-1-1988

Computer Data Banks and Personal Information: Protection Against Negligent Disclosure

Chris Dockrill
University of Alberta

Chris Dockrill*

Computer Data Banks and Personal Information: Protection Against Negligent Disclosure

I. *Introduction*

The common law has for centuries recognized the protection of certain interests which fall under the rubric of what is commonly referred to as the right of privacy.[1] While these safeguards have not always satisfied the concerns of the aggrieved individual, they have and continue to afford some measure of protection. The recognition of a need for a more specific means of protecting such interests is more recent in origin, dating to the later part of the last century.[2]

The concern for the privacy of the individual and the threatened intrusion made possible through the advances of technology, specifically that of electronic data-processing equipment (computers), is of even more recent origin. Developments in technology have brought about tremendous enhancement in the capabilities and an associated reduction in the cost of such equipment. This coupled with the growth in the volume and complexity of our everyday transactions, has given rise to a phenomenal spread of such equipment throughout the world. The inevitable result has been an ever-increasing impact on our daily activities.

The spread of computers had grown from the installation of the first few experimental models in the late 1940s and early 1950s to approximately 300,000 world-wide by 1974. However, in the last dozen years this number has increased to approximately 48 million[3] individual systems world-wide and is expected to continue at a similar pace for some time.

---

* LL.B., University of Alberta.

1. For instance, the torts of trespass, nuisance, defamation and besetting have afforded remedies to those who have felt that their sphere of privacy has been intruded upon.

2. *See* Godkin, *Scribner's Magazine,* July, 1890, at 65 and Warren and Brandeis, "The Right to Privacy" (1890), 4 Harv. L. Rev. 193.

3. To place these numbers in perspective it must be remembered that until the early 1970s only medium to large organizations could afford these devices. Through the development of new technologies, particularly LSI (large scale integration) and VLSI (very large scale integration) the physical size and cost associated with these devices have both dropped dramatically. These numbers represent not only the multi-million dollar systems installed in public and private sector organizations, but also the micro-computers with price ranges from under one hundred dollars to ten or fifteen thousand dollars, which may be found in many homes today.

Considerable attention has been paid by many writers to the impact of these devices upon our individual and collective rights of privacy. We are confronted daily with stories of threats which are posed by these intrusive devices. Both the news and entertainment media fill our lives with reports of actual and fictional occurrences which have stripped individuals of their protective shield and exposed them to the scrutiny of others.

The majority of these scenarios focus upon deliberate efforts of governmental agencies, cloaked within their administrative powers, to amass and utilize more and more information concerning individuals, or the illegal activities of individuals or organizations in acquiring access to similar information. Major concern has been focused upon intentional acts and their threat to the privacy of the individuals involved. Typical examples of such occurrences include:

(a) proposals within the United States during the early 1970s for the establishment of a National Data Centre;[4]
(b) the U.S. federal "Project Match",[5] under which the welfare rolls of the Department of Health, Education and Welfare are matched to federal payroll files[6] in an attempt to catch federal employees who were defrauding the welfare system;
(c) discovery,[7] by the Canadian federal government, of suspected tax evaders, and welfare and unemployment insurance cheaters through the computer matching of benefit payment records against records of employment and separation from employment, provided to the government for the purposes of administering various programs;
(d) the U.S. Department of Defence discovery of a discrepancy of 186,000 individuals, when they matched drivers license registration for 18-year-old males with draft registration files.

Throughout the literature, the shared concern appears to be about the growth in governmental powers in this area and the widespread development of private organizations[8] which collect and disseminate,

---

4. Such an undertaking would draw together all information concerning individuals held by governmental agencies and would, through correlation and matching techniques, make tremendous amounts of information available to those who had access to the files.
5. 43 Fed. Reg. 1135 (1978).
6. The U.S. Supreme Court has upheld special treatment of federal civil servants notwithstanding the constitutional guarantees of equal treatment before the law. *See: United Public Workers* v. *Mitchell* 330 U.S. 75 (1947) upholding restrictions on civil servants' participation in political campaigns.
7. J. Sallat, "Computer sleuthing leads Ottawa to millions in jobless overpayments", *Globe and Mail,* October 3, 1984.
8. Professor Miller speaks of the "information buddy system" whereby "the result is a subterranean information exchange network that functions on a mutual backscratching basis or

generally for a fee, both personal and financial information relating to individuals.

While these may represent legitimate interests, they are not the only matters with which we should concern ourselves. There is another less obvious but equally threatening aspect of the invasion of privacy which most often is totally ignored. This relates to breaches of confidentiality or disclosures of information, not as the result of a deliberate effort of any individual, but rather as a result of carelessness or negligence.

It is this aspect of the protection of privacy with which this paper is concerned. It will address the sources of such breaches or invasions, the remedies or relief available to those who are affected and will attempt to assess the current provisions for protecting against such occurrences. It will conclude with recommendations to ensure a greater measure of protection of the right of privacy of the individual.

II. *Legitimate Rights of Data Access*

> Privacy has been seen as a right which must, to a certain extent, be surrendered in return for social benefits.[9]

There can be no doubt that, faced with the nature and complexity of our daily activities, we have no alternative but to accept the presence of computers in our lives. Even the most adamant critics of the intrusion of computer systems must recognize the need for both private and public sector organizations to employ computers in the storage and processing of the information which is essential to their effective operation. Without the speed and economies of computer processing, the provision of many goods or services would be impossible or, at best, far more expensive.

If business organizations are going to extend credit, they must have the right to check the credit history of applicants. If government agencies are to use public funds, in the best interests of the public, they must have access to means of detecting and preventing fraud and abuse of their programs.

The legitimate use of such facilities has therefore become a recognized feature of our daily lives. The credit bureau files, department store accounts, our banking records, government files concerning every aspect of our lives, are all computerized. We accept this as a natural state of affairs. And so we should, so long as we are confident that these files contain accurate and timely information, nothing which is not relevant to

---

can be invoked for a fee". ("Computers, Data Banks and Individual Privacy: An Overview", [1972] 4 Colum. Human Rights L. Rev. 1 at 10).

9. S.J. Toope and A.L. Young, "The Confidentiality of Tax Returns under Canadian Law" (1982), 27 McGill L.J. 479 at 482.

the purpose for which they are maintained and that their contents are not disclosed to unauthorized individuals.

The objective of maintaining any file, whether manual or mechanized, is to serve some specific purpose. This purpose is generally to facilitate or prevent the occurrence of certain events. For instance, credit bureau files are ostensibly maintained to lessen the likelihood of individuals abusing the credit-granting system. Experience has shown that, even with computerized reporting systems, some abuses do occur.[10] The effect of such situations is an increase in costs to all consumers to cover these losses. Similarly, government programs must be monitored to ensure that abuses are prevented.

In order to achieve those ends, organizations must collect, store and utilize large volumes of information concerning the citizens with whom they deal. As a consequence of these activities, individuals who are employed by these organizations become privy to such information in the course of their employment.

These specific uses of information generally do not cause alarm unless a breach occurs. This information can, if used in other ways, create greater exposure for the individuals concerned. Examples of activities or proposals which have caused alarm include:

(a) a proposal to amend the Alberta Public Health Act to permit the disclosure of confidential information about persons with communicable and sexually transmitted diseases when it is in the public interest;
(b) examination of confidential medical records in an effort to catch doctors who may be cheating the Ontario Health Insurance Plan;[11]
(c) a proposal by the federal Solicitor General to give the new civilian security agency access to medical records to assist in their protection of national security;[12]
(d) the introduction of new legislation in Alberta to compel public agencies and individuals to release, to a court or designated individual, any information concerning the whereabouts of anyone who is delinquent in maintenance payments;[13]
(e) attempts by Revenue Canada to obtain confidential information on clients from a commodities futures market broker;[14] and

---

10. "Couple proved foreclosure not always financial suicide", *Calgary Herald,* June 18, 1984.
11. Public Health Act, R.S.A. 1980, c. P-27.
12. "Let spy-catchers use medical data: Kaplan", *Globe and Mail,* May 23, 1984.
13. "Support payment reforms ahead", *Edmonton Journal,* July 9, 1984. *See* Maintenance Enforcement Act, S.A. 1985, c. M-0.5.
14. *James Richardson and Sons Ltd.* v. *M.N.R.,* 84 D.T.C. 6325 (S.C.C.), *rev'g* 82 D.T.C. 6204 (F.,A.D.), *aff'g* 81 C.T.C. 229 (F.,T.D.).

(f) a proposal for the establishment of a computerized prescription registration system to curtail illicit drug trade in narcotics.[15]

These and countless other activities pose an even greater threat to the virtually non-existent rights of privacy.

III. *Nature of the Breach or Invasion*

Computers do not invade privacy. They are merely instruments which, when employed by their skillful and sometimes devious users, make possible the intrusion upon or invasion of the privacy of others. It must be remembered that it is the individuals behind these machines who are the source of that intrusion.

Notwithstanding the general level of awareness of computers among the public, there are still many misconceptions which abound. One of these, perhaps even fortified by the awareness of and experience with micro-computers, is the false impression of the use and operation of large computer systems.

The belief that the system is operated and controlled by one or two individuals who have control of the "big button" which gives them access to all of the computers' secrets is far from reality. The operation of computer systems involves many individuals, with large organizations typically having hundreds of staff employed exclusively in some facet of its data-processing activities. Accordingly, any or all of these individuals may, to some degree, have access to the information which is processed and stored by these computer systems. These individuals may be engaged in any number of activities, including preparation and entry of the data for processing by the computers; creation of the programs which perform the processing functions; operation of the hardware and its peripheral components; or even the delivery of printed reports produced by the computer to the users of such information. Ironically, those who operate the computer hardware often have the least access to the data which it is manipulating. It is the users of that information, scattered throughout the organization, who have the greatest access.

There is also a general misconception of the level of security surrounding the accessibility of information which is stored by computers. Most people are familiar with the security measures which are utilized within the data-processing environments. We hear of cipher

---

15. "Doctor-shopping drug scam on increase", *Edmonton Journal,* June 25, 1985. *See: Whalen* v. *Roe,* 429 U.S. 589 (1977) where a similar scheme was found not to be an undue invasion of privacy since access was limited to appropriate officials. This program has been developed and has resulted in the detection of patients and physicians suspected of abusing controls on certain drugs.

locks on the physical premises of data centres, cryptic passwords which are employed by authorized users to identify themselves to the computer before it will permit access to its resources and data encryption techniques which are used to render useless any data which falls into the hands of unauthorized individuals. But in spite of all these precautions, breaches do occur.

The old adage that a chain is only as strong as its weakest link is most appropriate in this regard. One writer has stated:

> . . . if you walk into a hospital you will often find case notes lying around. It would be an easy matter to pick them up and read them. The security of the information held in a computer is much greater.[16]

While this observation is entirely accurate, it perhaps ignores a major aspect of the use of the computers for information processing and storage. There is no value in merely storing information. It is stored so that it may be later retrieved and used for some constructive purpose. The two main ways in which such information is retrieved is either through display on a video terminal or via a hardcopy printer. In the first instance, the information is temporarily displayed[17] and, once the image leaves the screen, is no longer accessible unless displayed in response to another authorized request. In the latter instance, the information remains on the printed page, accessible to anyone who may gain access to that piece of paper, until it is destroyed. Information stored in computers can also take other forms. Computer Output Microforms (COM) is a common method for handling such information. A number of recent incidents of unauthorized disclosure of information, involving microfiche, highlights the vulnerability of such information sources.

We, as users of these sophisticated computer systems, tend to stress the "high-tech" security measures yet often overlook the obvious sources of potential compromise of data security.

Consider the following scenarios:

(a) A computer programmer has just completed the development of a new system (series of computer programs) which, when in operation, will process the accounts receivable for a business concern. As the last step in the development of the system, the programmer must thoroughly test the programs. To provide the data for this test, he sits down with the local

---

16. N. McIntyre, "Medical Records: Computers and the Patient" (1982), 50 Medico-Legal J. 159 at 165.

17. Some systems are designed to display the requested information until a subsequent request is made by the user. In such instances it is possible that a particular display may be left on the screen for an extended period of time.

telephone directory and pulls names and addresses at random[18] using these as the basis of his test data. After running his tests, he discards the results, which somehow fall into the hands of someone who knows one of the individuals who appears on this list and tells the test subject that he is surprised to see that that individual has such a bad credit record.
(b) The same circumstances occur as above, except in this instance the programmer uses real data from the organization's files.[19]
(c) An individual employed by Revenue Canada (or for that matter any other agency having access to income tax files[20]) is curious about the income level of a prominent citizen in the community, a sports celebrity or a friend. He looks at the file which he normally would have no need to reference.
(d) A copy of a credit rating report is found lying in an alley next to the garbage bin of a commercial credit bureau.[21]
(e) Through an error in processing, the computer system of a credit-reporting agency provides erroneous data concerning an applicant for credit. As a result, the applicant is refused and suffers humiliation and embarrassment.

While each of the foregoing examples represents a potential intrusion into the privacy of the individual or individuals involved, they are only a small part of the number of similar activities which occur daily. Characteristic of each of these scenarios is the absence of malice[22] on the

---

18. This is a very common practice in the data-processing community. While working as a systems analyst for a provincial government department during the late 1960s, a colleague seriously jeopardized his career through a similar practice. He was working on a public health system and chose the names of the management and staff of the office in which he worked. He made the further mistake of leaving the results of his tests on his desk to be seen by all who wandered by. Needless to say, his supervisor was not amused by the combination of venereal diseases which had been attritubed to him in this test data.
19. Since this is only a test there is likely to be little concern about the disposal of the results.
20. The McDonald Commission inquiry into the R.C.M.P. uncovered the fact that Revenue Canada routinely gave tax information to the R.C.M.P., although they had no legal right to do so without following established procedures. Laycraft J. of the Alberta Bench, in his inquiry into the operations of Royal American Shows Inc., pointed to the ineffective definitions regarding the provisions of confidentiality of tax return information in s. 241 of the *Income Tax Act.*
21. Documents, including computer printouts of savings and chequing accounts for credit union customers, and some papers containing personal information about the character of borrowers, were found outside a building in Winnipeg once owned by the Credit Union Stabilization Fund. *See* "Scramble for documents left in bin", *Edmonton Journal,* June 3, 1984. *See also* "Farm records found in garbage", *Edmonton Journal,* June 30, 1984.
22. In *The Assault on Privacy* (*infra,* note 61), at p. 33 Professor Miller states:

> Unthinking people are as capable of injuring others by unintentionally rendering a record inaccurate, losing it, or disseminating its contents to unauthorized users as are people acting out of malice or for personal aggrandizement.

part of the perpetrator and generally a situation where authorized access to the information in question did exist. It is this type of careless or negligent invasion of the privacy of others which poses just as great, and perhaps an even more prevalent threat to privacy than is evident from the deliberate acts of those who seek to intrude.

In response to a federal task force study questionnaire,[23] nearly one-third of the organizations which responded admitted that they did not employ any procedures or rules for disposal of data after its usefulness to the organization had passed.

The obvious questions which should arise in regard to each of these scenarios concerns whether or not citizens are protected against such breaches of or intrusion into their privacy. With some minor exceptions,[24] Canadian courts, unlike their U.S. counterparts, have not recognized a specific right of privacy. The next section of this paper explores this situation to determine the extent to which the right of privacy does exist in Canadian jurisdictions.

IV. *The Right of Privacy in Canada*

Unlike the strong U.S. experience,[25] the Anglo-Canadian common law tradition does not recognize a general right of privacy.[26] Although some statutory provisions exist in British Columbia, Saskatchewan, Manitoba, Quebec and Newfoundland,[27] not all provinces have seen fit to follow their lead. However, even those provinces which furnish a measure of statutory protection impose limitations on the protection which is afforded and the remedies that are available.[28]. Accordingly, those seeking legal protection of their privacy must look elsewhere and can expect varying treatment before the law, depending upon their place of residence.

---

23. *Privacy and Computers,* Report by The Department of Communications/Department of Justice 1972; question 20.A.5 at p. 214.

24. *Capan* v. *Capan* (1980), 14 C.C.L.T. 191 (Ont. H.C.); *Saccone* v. *Orr* (1981), 34 O.R. (2d) 317, 19 C.C.L.T. 37 (Co. Ct.). *See also: Motherwell* v. *Motherwell* (1977), 1 A.R. 47, 73 D.L.R. (3d) 62 (C.A.).

25. The recognition of the general right of privacy is generally credited to the influence of the Warren and Brandeis article, *supra,* note 2, followed by the first judicial recognition of such a right in *Pavesich* v. *New England Life Ins.,* 50 S.E. 68 (S.C. Ga. 1905) and later by cases such as *N.A.A.C.P.* v. *Alabama ex rel. Patterson,* 357 U.S. 449 (1958).

26. *See, e.g.,* J. Williams, "Invasion of Privacy" (1973), 11 Alta. L. Rev. 1.

27. R.S.B.C. 1979, c. 336; R.S.S. 1978, c. P-24; S.M. 1970, c. 74, S.N. 1981, c. 6; *see also* Art. 1053 of the *Quebec Civil Code.*

28. For example, both the B.C. and Saskatchewan statutes require willful conduct on the part of the defendant while the Manitoba statute requires substantial and unreasonable conduct, although none requires proof of damage to permit recovery. On this basis, in B.C. and Saskatchewan, and perhaps even in Manitoba, recovery would be precluded, for negligent acts regardless how outrageous the behavior was.

Professor Prosser[29] identified four distinct types of invasion:

1. intrusion upon the plaintiff's physical and mental solitude or seclusion;
2. public disclosure of private facts;
3. publicity which places the plaintiff in a false light in the public eye;
4. appropriation, for the defendant's benefit or advantage, of the plaintiff's name or likeness.

This examination is concerned with categories 2 and 3 only. These represent the class of activities which are evident in the examples cited in the previous section. Both deal with the disclosure or publication of facts or information concerning another individual. In numerous judgments, the U.S. courts have held that the publication of personal or confidential information, concerning another, is actionable whether under the head of invasion of privacy[30] or under some other cause of action, such as breach of confidence,[31] but have stopped short of affixing liability where that which has been disclosed is already a matter of public record.[32]

What, then, is the Canadian stand on such matters? In the foregoing examples of an invasion, by way of disclosure, the aggrieved party is not entirely without remedy. The remedies which are available to that individual include possible tort or contract actions as well as the possibility of an action under a provincial or federal statute. We will assess each of these alternatives in turn.[33]

1. *Defamation*

It is well accepted that an action for defamation will lie where the defendant committed the act or acts complained of with no intention to defame or where he had no knowledge of the plaintiff.[34]
Therefore, the negligence of the defendant is sufficient to create liability.[35]

---

29. W.L. Prosser and J.W. Wade, *Cases and Materials on Torts,* (5th ed. 1971) at 930.
30. *Melvin* v. *Reid,* 112 Cal. App. 285; 297 P. 91 (4th Dist. C.A. 1931).
31. *Peterson* v. *Idaho First Nat. Bank,* 83 Idaho 578; 367 P. (2d) 284 (1961).
32. *Melvin* v. *Reid, supra,* note 30, *Meetze* v. *Associated Press,* 230 S.C. 330; 95 SE 2d 606 (So. Car. Sup. Ct. 1956).
33. This discussion of possible remedies is not intended to be definitive in scope. It is intended to address some of the possible avenues of redress for the party who feels that his privacy has been invaded or compromised. This coverage focuses upon the general applicability of each remedy and its possible strengths and inherent limitations in addressing the needs of such individuals.

Obviously, issues such as causation, remoteness, foreseeability and the interplay of defences such as *novus actus interviens* play a major role in the success of any legal action which is initiated in response to such intrusions into privacy. Due to the limitations of space, a more detailed discussion of the individual elements of each remedy is not possible.
34. *E. Hulton & Co.* v. *Jones,* [1910] A.C. 20 (H.L.).
35. *Cassidy* v. *Daily Mirror Newspapers Limited,* [1929] 2 K.B. 331 (C.A.).

Success in this regard is, however, tied to the proving of defamation and not to the mere publication of the facts or information. This will require that the facts complained of be shown to be:

> . . . calculated to bring [the plaintiff] into hatred, ridicule or contempt . . . or causes [him] to be shunned or avoided.[36]

It must be remembered, however, that the defendant may avail himself of certain defences. Paramount among these is the defence of justification (or truth).[37] Therefore, it would seem that, for the plaintiff to succeed in an action for defamation, the facts disclosed must be entirely fabricated or sufficiently incorrect to satisfy the requirements of injury to the plaintiff's reputation or standing in the community.[38]

It can be seen that there is some potential for redress in this area although it will be limited by the circumstances of the publication or disclosure of the information.

2. *Breach of Confidence*

An action for breach of confidence will likely give rise to several problems. Foremost among these is the fact that the courts are prone to limit this action to commercial relationships[39] and require that an explicit reliance has been established between the parties.[40] The remedy in such situations is generally limited to an equitable injunction, unless substantial economic loss has been incurred. In many instances, the courts have been reluctant to give relief even in the face of deliberate disclosures of personal information.[41]

In establishing the action for breach of confidence, the plaintiff must prove a reasonable expectation of privacy existed between him and the defendant. The U.S. courts have been quite harsh in refusing to accept a claim of reasonable expectation of privacy.[42]

---

36. *Youssoupoff* v. *Metro-Goldwyn-Mayer Pictures Ltd.* (1934), 50 T.L.R. 581 (C.A.).
37. Under the circumstances, availability of other defences such as consent is also significant.
38. Notwithstanding that under statute, in most jurisdictions, an action for defamation may proceed without proof of damages, courts are likely to award successful plaintiffs nominal damages unless substantial harm can be established: *Murphy* v. *La March et al,* [1971] 2 W.W.R. 196 (B.C.C.A.); *aff'g.* (1970), 73 W.W.R. 114 (B.C.S.C.).
39. *Pre-Cam Exploration and Dev. Ltd.* v. *McTavish,* [1966] S.C.R. 551, where a constructive trust was found to exist.
40. *Deeks* v. *Wells,* [1933] 1 D.L.R. 353 (P.C.)
41. *Doe* v. *McMillan,* 459 F. 2d 1304; *rev'd in part* and *aff'd in part* 412 U.S. 306 (1972).
42. *See, eg.: United States* v. *Miller,* 425 U.S. 435 (1976); *Burrows* v. *Superior Court of San Bernardino County,* 13 Cal. 3d 238; 529 P. 2d 590 (Cal. Sup. Ct. 1974) and *Charnes* v. *DiGiacomo,* 612 P. 2d 1117 (Col. Sup. Ct. 1980). The U.S. Congress responded to the decision in *U.S.* v. *Miller* by passing the Right to Financial Privacy Act of 1978 (12 U.S.C. 340 Supp. II 1978) which has given at least a limited measure of protection (*Hancock* v. *Marshall,* 86 F.R.D. 209 (Dist. Ct. D.C. 1980).

As with the action for defamation, the likelihood of a plaintiff succeeding under this head is remote unless there exists a verbal or written agreement, between that individual and the data base owner, which gives an assurance of privacy, sufficient to cover any of these situations. Given the relative bargaining strength of governmental and commercial establishments in their dealings with the public, it is highly unlikely that such an undertaking would ever exist.

Breach of confidence should not be ruled out without some consideration, but, as one writer has stated:

> . . . in as much as the action of breach of confidence has served to protect knowledge, attributes and information, it does not logically give rise to a good argument supporting privacy in the sense of protecting the sensibility and dignity of the individual.[43]

3. *Negligence*

Unless the plaintiff can show tangible evidence of damages (*i.e.*, loss of employment or injury to financial standing) the likelihood of recovery under this cause of action is virtually non-existent. The plaintiff must also establish negligence, with the particularly difficult task of showing the existence of a duty of care. Even where a statutory duty of non-disclosure exists,[44] in light of the Supreme Court decision in *In Right of Canada* v. *Saskatchewan Wheat Pool*,[45] it is unlikely that any successful action may be brought unless a duty can also be shown to exist at common law.

The strongest arguments for finding the requisite duty of care will no doubt arise in those circumstances where the complainant is participating in a non-volitional capacity or where express or impled contractual terms of non-disclosure may be found to exist.

Given the state of the art in data-processing technology, and the individual's general inability to be familiar with the techniques and procedures employed by large organizations, there is a strong case to be made for the application of the doctrine of *res ipsa loquitur*. This will be particularly true where there is any suggestion of the "problem" arising from a computer software error.

In the absence of inside information, it will be virtually impossible for a plaintiff to identify specific acts of negligence which are the basis of the claim being asserted. A plaintiff could experience difficulty in attempting to prove negligence without a detailed knowledge of the intricacies of the offending organization's information-processing systems. Because of the

---

43. Glasbeck, "Limitations on the Action of Breach of Confidence", in Gibson, ed., *Aspects of Privacy Law* (Toronto: Butterworths, 1980) at 227.
44. *See, eg.* s. 241 of the *Income Tax Act*, R.S.C. 1952, c. 148.
45. [1983] S.C.R. 205

concern for the potential vulnerability of their information resources, most organizations have taken precautions to limit access to and knowledge of their information-processing facilities. Often, the nature of some acts is such that there is no tangible evidence of negligence. If the circumstance arose from an error in a computer program, the plaintiff will, no doubt, experience difficulty in gaining access to that program. If he does succeed, the error will likely have been corrected and no trace will have been left. Often, the nature of the problem itself is such that evidence of negligence is destroyed by the computer system.[46] Since much of this information is recorded in electronic form, it is readily destroyed without any trace.

Where all such information is in the sole possession of the defendant, and it is highly probable that the problem arose from the negligence of the defendant, it is unjust to merely permit the defendant to demur or insist that the plaintiff provide more specific allegations.[47] It must not, however, be assumed that *res ipsa loquitur* applies automatically in all instances where advanced technology is employed. Obviously, the requirements set out in the case law since *Byrne* v. *Boadle*[48] must be satisfied.

4. *Conversion*

A more controversial action would be one for conversion. Again the question of a non-deliberate act may arise, but this is no bar to an action for conversion.[49] Similarly, the fact that the disclosure arose from a negligent act does not preclude liability attaching to the defendant.

In any action for conversion relating to disclosure of information, there are two major hurdles to overcome. The first relates to whether the law recognizes property rights in information which are worthy of protection, and the second, to the concept of the ownership of the data or information.

(a) *Property in Information*

The courts have long struggled with the question of whether or not there is property, worthy of legal protection, in information. As early as 1918[50] the U.S. Supreme Court recognized a quasi-property interest in news

---

46. *Siegler* v. *Kuhlman*, 502 P. 2d 1181 at 1185 (Wash. Sup. Ct. 1972).
47. *Neal* v. *U.S.*, 402 F. Supp. 678 at 680 (D.N.J. 1975).
48. (1893), 2 H. & C. 722; 159 E.R. 299 (Ex. Ct.).
49. *Hollins* v. *Fowler* (1975), 44 L.J.O.B. 169; 33 L.T. 73.
50. *International News Service* v. *Associated Press*, 248 U.S. 215 (1918). Ironically, Justice Brandeis, who co-authored the seminal article on privacy with Samuel Warren, dissented in this judgement.

reports which had been copied by a competitor. Subsequent decisions also have recognized property rights in materials such as bank records.[51]

It is important to consider the Canadian courts' treatment of this subject in recent years. In the Ontario High Court, Krever, J., in *R.* v. *Stewart*,[52] ruled that confidential information is not property for the purpose of the law of theft. He reasoned that there must be some deprivation of the public or some individual of something of value. In this instance the accused had been charged with counselling theft contrary to s. 422 of the *Criminal Code*. It was alleged that he had importuned an employee to obtain a copy of the names of all the staff of the Constellation Hotel in Toronto. The information was to be used in an attempt to unionize the staff. As taking a copy did not deprive the hotel of its original property, Mr. Justice Krever concluded that no theft had occurred and therefore no crime had been committed.

The Ontario Court of Appeal reversed the judgement and entered a conviction[53] against the respondent. In doing so the court did not challenge the logic of Krever's J. finding. Rather, as stated by Houlden J., the court held:

> While clearly not all information is property, I see no reason why confidential information that has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purposes of its business should not be regarded as property and hence entitled to the protection of the criminal law.[54]
>
> To sum up, I am of the opinion that the confidential information of its employees compiled by the Constellation Hotel was property . . . [55]

Cory J. concurred:

> Lists compiled for business purposes fall within the term "literary works" and they are a proper subject-matter for copyright.[56]

While the reference to copyright protection may be *obiter*, there can be no mistake that this judgment is, for the time being, limited in application to commercial environments and the commission of criminal offences. As a result, the application of the principle of property in information to a tortious action in conversion, while an intriguing case to argue, may not be well received by the courts.

---

51. *Brex* v. *Smith*, 146 A. 34 (N.J. Ct. Ch. 1929).
52. *R.* v. *Stewart* (1982), 38 O.R. 89; 68 C.C.C. (2d) 305 (H.C.).
53. *R.* v. *Stewart* (1983), 42 O.R. (2d) 225; 5 C.C.C. (3d) 481 (C.A.).
54. (1983), 42 O.R. (2d) 255 at 236.
55. *Id.*, at 240.
56. *Id.*, at 244.

It is worth noting, in passing, that Mr. Justice Lacourciere wrote a rather compelling dissent in which he emphasized the statement of Krever J. at trial:

> It is not for a court to stretch the language used in a statute dealing with the criminal law, to solve problems outside the contemplation of the statute.[57]

He noted that Parliament was considering proposals[58] to extend the definition of property in the *Criminal Code* to expressly include computer data and software.

While this latter fact may improve the level of protection afforded to information stored within computer systems, it does not adequately address the issue of an individual's right to protect information concerning himself.

The *Stewart* case is now before the Supreme Court of Canada. While the outcome of the case may have little real impact on Mr. Stewart, (he received an absolute discharge when he appeared before Krever J. for sentencing, after the Court of Appeal handed down the guilty verdict), many individuals expect this case to establish new law. One must not lose sight of the significance of Krever's J. comments, cited above. The role of the judiciary is to interpret and apply the law, not to make the law. That responsibility lies with our elected members of Parliament or provincial legislatures, as appropriate.

In 1985, the federal Parliament amended the *Criminal Code* (ss. 301.2, 387) and created a new series of offences. These new offences related to the unauthorized use of computers or computer-based data. While these provisions cover a previously identified gap in the *Criminal Code*,[59] it is submitted that they do not automatically address the issue which arises in the *Stewart* case. Somewhat ironically, the scenario would be covered if the data or information were in "computer-processable" form. However, if it is merely recorded on paper, it appears not to be protected by these provisions. A stealthy and cautious individual could avoid the sanctions by carefully accessing the information at the appropriate point.

The issue which remains to be addressed relates to the value of information, regardless of its form or format of storage. If information is worthy of protection, it is worthy in all forms. It is submitted that this is the basic issue, not whether "computer-processable" information

---

57. *Id.*, at 230.
58. Bill G 667, 1st Session, 32nd Parl., 1980-81-82.
59. *R.* v. *McLaughlin,* [1980] 2 S.C.R. 331; 23 A.R.2d 30; *aff'g.* (1979), 19 A.R. 368; 51 C.C.C. (2d) 243 (C.A.).

deserves protection. Considerable unnecessary problems could be avoided, including the need for our courts to struggle with such issues, if our legislators were more proactive and less reactive in their approach.

(b) *Ownership*

The plaintiff's case for ownership of information regarding himself is perhaps stronger where the defendant has misappropriated it (*i.e.*, where it has not been given willingly by the plaintiff). Accordingly, his case would be much stronger in those instances where the individual involved (the programmer in our examples) had merely culled it from the telephone directory or other similar sources. However, in those instances where the information arose from public sources, like telephone directories, the courts would likely be hesitant to recognize the plaintiff's right to claim an exclusive interest in the information.[60] It has been suggested[61] that we might want to consider information about ourselves in the same light as a picture and accordingly seek the same protection for data that we afford under the action for appropriation, for gain, of the likeness or image of another. Any such attempt would, however, be administratively untenable and impossible to live with.

The cases which have been decided in this area (*i.e.*, ownership of data) tend to support the concept of ownership in the individual who has expended energy in its collection.[62] This unfortunately weakens the case for the victim of the disclosure.

5. *Mental Suffering or Nervous Shock*

In the majority of circumstances arising from the factual situations being addressed here, the injury complained of will not involve any physical harm to the complainant, nor to his or her property. In most instances the harm will be limited to the distress and embarrassment arising from the revelation of what are considered private facts concerning that individual.[63]

Traditionally, the courts have been hesitant to award compensation for mental suffering, particularly in the absence of any physical harm.[64]

---

60. *See: Melvin* v. *Reid, supra,* note 30.
61. A. Miller, *The Assault on Privacy,* (The University of Michigan Press: Ann Arbor, 1971).
62. *Seager* v. *Copydex Ltd.,* [1967] 2 All E.R. 415 (C.A.).
63. *See* Prosser's second category, *supra,* note 29. It is possible, however, that a complainant may have suffered economic loss. This may arise where the plaintiff has incurred costs or lost the benefit of a transaction as a result of the defendant's negligent release of the information. *Cf. Dun & Bradstreet* v. *Greenmoss Builders Inc.,* 105 S.Ct. 2939 (1985).
64. *Wilkinson* v. *Downtown,* [1897] 2 Q.B. 57; *Abramzik* v. *Brenner* (1967), 65 D.L.R. (2d) 651 (Sask C.A.); *Bourhill* v. *Young,* [1943] A.C. 92 (H.L.).

There has been some lessening of this practice, particularly in Ontario, in regard to wrongful dismissal cases.[65] There may also be problems associated with establishing causation and foreseeability of the harm. It should be noted, however, that if such a cause of action can be established, recovery need not be limited by the lack of physical damage or loss. Canadian courts have generally not accepted the restriction of *Rookes* v. *Barnard*.[66] Accordingly, it may be possible for a plaintiff to argue for substantial exemplary damages, in Lord Devlin's words, "whenever it is necessary to teach a wrongdoer that tort does not pay."[67] This will depend upon showing outrageous behavior, or neglect, on the part of the defendant.

One basis for mounting an argument in favour of an embarrassed plaintiff may be based upon § 46 of the *Restatement of Torts, Second* which specifies:

> One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress . . .

While the *Restatement* is merely a guideline to United States law, Canadian jurists often look to such sources in difficult circumstances.

Admittedly, the scenarios being discussed here are unlikely to fit the requirements of the established law. However, given the paucity of protection afforded to such plaintiffs it is necessary for their legal agents to seek out imaginative arguments in support of their protection.

6. *Breach of Contract*

Much of the information provided to others occurs in the context of business transactions between the parties. It will be rare to find express contractual protection for the confidentiality of such information, particularly considering that the transaction generally occurs under terms and conditions specified by the recipient of such information.[68] Where such terms do exist, an action for breach of a contractual term is appropriate.

---

65. *Cf.: Pilon* v. *Peugeot Can. Ltd.* (1980), 114 D.L.R. (3d) 378; 29 O.R. (2d) 711 (Ont. H.C.); *Pilato* v. *Hamilton Place Convention Centre Inc.* (1984), 7 D.L.R. (4th) 342 (Ont. H.C.). *See also: Jarvis* v. *Swan Tours Ltd.,* [1973] 1 Q.B. 233; [1973] 1 All E.R. 71 (C.A.).
66. [1964] A.C. 1129 (H.L.).
67. Id., at 1227.
68. Tenants, employees, bank depositors, taxpayers and applicants for government benefits must generally comply with the demands of the other party or forgo the transaction. The lack of voluntariness of customers in supplying information to banks played a key role in the suppression of such evidence obtained from the bank in *Burrows* v. *Superior Court of San Bernardino County,* 529 P. 2d 590 (Calif. S. Ct. 1974).

Absent express provisions, or in the face of limitation of liability, waiver of liability or liquidated damages clauses, a potential plaintiff is not without redress. The courts have struck down such limiting provisions but in recent years, only where oppressive [69] or unconscionable behavior has been exhibited. It is submitted that plaintiffs will have to show that they were placed in a position where they had no option but to accept the other party's one sided conditions. Even in such instances, courts are likely to rely upon the principle of freedom to contract (or not contract).

Another possibility arises from the courts' willingness to imply contractual terms of non-disclosure in certain relationships. The keystone case in this area is *Tournier* v. *National Provincial and Union Bank of England.*[70] The plaintiff was the recipient of a cheque from another customer of the same bank with which he dealt. Rather than paying the funds into his account, he endorsed the cheque to a third party. When the cheque was cleared through the bank, the manager made enquiries through the bank in which the cheque had been deposited. Upon being informed that the endorsee was a bookmaker, the manager disclosed this information to the plaintiff's employer. The plaintiff was dismissed and brought an action for breach of an implied contractual term of confidentiality. It appears that the bank manager was motivated by the fact that the plaintiff had ceased to make the agreed-upon installment payments on the overdraft in his account. On appeal, of a judgment in favour of the respondent, the court ordered a new trial and indicated that the bank owed a qualified duty of non-disclosure to its clients. Bankes L.J. stated that disclosure on "a reasonable and proper occasion" was permissable only when compulsion by law, duty to the public, the interests of the bank, or express or implied consent of the depositor warranted.[71]

Tournier was followed in *Hull* v. *Childs and The Huron and Erie Mortgage Corporation.*[72] Gale J. held that the institution had breached its implied duty of non-disclosure but did not give judgment against the defendant because the loss was not caused by this breach.[73]

Tournier suggests a judicial concern for the protection of the client's financial interests. Whether such a duty can be extended to protect the dignity and privacy of the individual is untested and therefore uncertain.

---

69. *See* Dickson J.'s comments, as he then was, in *Elsley* v. *J.G. Collins Ins. Agencies Ltd.*, [1978] 2 S.C.R. 916 at 937.
70. [1924] K.B. 461 (C.A.).
71. *Id.*, at 473.
72. [1951] O.W.N. 116 (H.C.). *See also: Suburban Trust Co.* v. *Waller,* 408 A. 2d 758 (Md. Ct. Spec. App. 1979).
73. As noted previously, issues such as causation and remoteness may be significant.

7. *Breach of a Fiduciary Obligation*

In a fashion similar to the imposition of implied terms of good faith and fair dealing in contracts, equity imposes a number of obligations upon those who are placed in a fiduciary relationship relative to others. Whether such a relationship and its concommitant duties are sufficient to protect the interests which this paper addresses is uncertain. Obviously, this avenue of redress will be open only where the relationship in question is one to which a fiduciary obligation attaches.

From a review of the case law, it would appear that personal or confidential information may be afforded some measure of protection. In *Re Londonderry's Settlement*,[74] Salmon L.J. held that a beneficiary has a proprietary interest in trust documents. In *Re Smith*,[75] McRuer C.J. found that a beneficiary's interest in information relating to the trust was based upon his proprietary interest in the *res* of the trust. In both instances, the issue before the court was the beneficiary's right to inspect trust documents. Both cases held that the *cestui que trust* has such a right, but that a trustee has the right to withhold information relating to the trustee's discretionary powers so as not to render the duty of administration impossible. While both of these cases stand for the proposition that a beneficiary has a right of access, they do not automatically equate to a right of privacy. This principle will require persuasive argument.

The existence of a proprietary interest worthy of protection appears to be a critical element in finding judicial support for protection against disclosure. While protection flowing from a fiduciary relationship may be limited, there is still the possibility that the court may be persuaded that such protection is warranted. This may require demonstrating to the court that disclosure has placed or could place the claimant in financial or emotional jeopardy. It is also worth noting that there is judicial recognition of the fact that the categories of cases, and the nature of the relationships, which will give rise to fiduciary obligations are not closed.[76]

Fiduciary obligations will attach to a number of relationships where individuals or organizations possess or control information concerning others. These include dealings with banks or other financial institutions, lawyers, financial advisors, corporate officers and some public officials. Whether or not the plaintiff can fit his situation into the technical requirements of a fiduciary relationship will depend upon the specific

---

74. [1964] 3 All E.R. 855 (C.A.).
75. [1952] O.W.N. 62 (H.C.).
76. *Cf.: Laskin* v. *Bache & Co. Inc.*, [1972] O.R. 465; 23 D.L.R. (3d) 385 (C.A.); *Evans* v. *Anderson* (1977), 3 A.R. 361; 76 D.L.R. (3d) 482 (C.A.); leave to appeal to S.C.C. refused (6 A.R. 270).

circumstances. A basic element of this relationship requires that one party be placed in the position of dealing with the interests of another in confidence and with scrupulous good faith and candor. There would be a much stronger legal argument to be advanced if judicial recognition of personal information as an asset existed. In the absence of this vital factor, a plaintiff may be limited to those situations where the disclosure of information occurred in the course of dealing with other assets. Since many individuals in the business community do not recognize the true value of information as an asset, it should not be surprising to find limited legal recognition.

Even where the action succeeds, the scope of available equitable remedies may be somewhat limited in dealing with the type of breach that is likely to arise. For instance, injunctive relief will be of no benefit after the fact and therefore will be limited to suppression of such disclosures when they are known in advance.[77]

Similarly, remedies such as accounting, tracing and the use of a constructive trust all require a proprietary interest which, as previously indicated, may not exist in the information which is the subject of concern.

8. *Strict Liability Under* Rylands *v.* Fletcher

In 1868, the House of Lords held that certain conduct, whether or not it was wrongful *per se*, was so unusual in a particular community, or attracted such a level of danger, that the risk of harm to others should be borne by the individual who engaged in that conduct.[78]

On any traditional analysis of the principle set out in this case it would be impractical to consider the application of this doctrine to any of the scenarios described earlier. The language of *Rylands* v. *Fletcher*, and many of the cases which followed its *ratio*, speak in terms of dangerous,[79] ultra-hazardous[80] or abnormally dangerous[81] activities and of non-natural use of land[82] and of "escape"[83] from the land.

It would be ludicrous to suggest that the use of computer systems to collect and manipulate data was a dangerous or non-natural use of land *per se*. It must also be remembered that the principle of strict liability

77. *Glover* v. *Bell Canada,* [1981] 2 S.C.R. 563; 130 D.L.R. (3d) 382; *aff'g.* (*sub nom. Glover* v. *Glover (No. 2)*) (1980), 29 O.R. (2d) 401; 113 D.L.R. (3d) 174 (C.A.).
78. (1868), L.R. 3 H.L. 330 (H.L.).
79. *Fletcher* v. *Rylands* (1866), L.R. 1 Ex. 265, *per* Blackburn J.
80. *Restatement of Torts,* § 520 (1938).
81. *Restatement of Torts, Second* § 519 (1977).
82. *Rylands* v. *Fletcher, supra,* note 78 *per* Lord Cairns; *Rickards* v. *Lothian,* [1913] A.C. 263 (P.C.).
83. *Read* v. *J. Lyons & Co. Ltd.,* [1947] A.C. 156 (H.L.).

developed in *Rylands* v. *Fletcher* is a variant of trespass and nuisance actions, whose purpose is to protect property interests. Once again the non-proprietary nature of information stands as a potential obstacle to recovery.

Like so many other areas of the law, the strict liability doctrine of *Rylands* v. *Fletcher* has been adapted to changing needs. In Canada the principle is at best uncertain. The Supreme Court of Canada has held that there is no necessity to prove unusual or non-natural use of land; a showing of increased risk of harm is sufficient to establish liability under *Rylands* v. *Fletcher*.[84] A number of other decisions have reinforced this position expressly or indirectly through avoidance of the use of the traditional language.[85] On the other hand, a number of cases have insisted upon applying the literal interpretation of *Rylands* v. *Fletcher* and refused to find liability in the absence of both non-natural use and escape.[86]

It is submitted that there is a credible argument to be made in support of the application of the *Rylands* v. *Fletcher* principle to the negligent disclosure of information from computer based information banks. In most cases of unauthorized disclosure, there has been an "escape" of the information. Whether it was through insufficient security precautions, which led to unauthorized access, or carelessness in the handling and disposal of information, the result has been the release or "escape" of information. One need not look far to recognize the value of controlling or manipulating information. In the early 19th century, large fortunes were made by those who had advance knowledge of Napoleon's defeat at Waterloo. Today, the incidence and the magnitude of insider trading profits are astounding. It is surely time that we recognized the inherent dangers associated with careless handling of information.

The computer systems and other mechanisms which speed our information handling must be subjected to some means of control. These facilities not only enhance our ability to process more information for positive purposes, they increase our vulnerability to inappropriate disclosure or use of information. This increased risk could provide the basis for arguing application of the *Rylands* v. *Fletcher* principle.

It has long been accepted that the burden of increased risk should be borne by the organization or individual who has created that risk. The

---

84. *Crown Diamond Paint Co.* v. *Acadia Holding Realty Ltd.*, [1952] 2 S.C.R. 161.
85. *Bliss and Bliss* v. *Heimbecker and Barker* (1982), 35 A.R. 280 (Q.B.); *Newell* v. *R.E. Newell Fisheries Ltd. et al.* (1982), 54 N.S.R. (2d) (S.C.T.D.); *Metson* v. *R.W. DeWolfe Ltd.* (1980), 43 N.S.R. 221; 14 C.C.L.T. (S.C.T.D.).
86. *Maron et al.* v. *R.A.E. Trucking* (1981), 31 A.R. 216 (Q.B.); *Lyon et al.* v. *Village of Shelburne* (1981), 130 D.L.R. (3d) 306 (Ont. Co. Ct.); *but see: Fingas* v. *Summerfield Colony* (1980), 5 Man. R. 361 (C.A.).

commercial value of the enterprise and the social responsibility of shifting the burden to the creator of the risk is best demonstrated by the words of Bramwell L.J.:

> It is just and reasonable that if a person uses a dangerous machine, he should pay for the damage which it occasions; if the reward which he gains for the use of the machine will not pay for the damage, it is mischievious to the public and ought to be suppressed, for the loss ought not to be borne by the community or the injured person.[87].

The inappropriateness or abnormal risk need not be associated with the activity in question but may be related to the means employed in carrying it out.[88] But even where a court requires the use of the traditional language, it could be demonstrated that the harm complained of was caused by the escape of information and that there is a potential risk of great harm associated with such occurrences.[89]

Given that the damages will generally be limited to emotional distress or pure economic loss, it will be necessary to persuade the court that such losses are recoverable under *Rylands* v. *Fletcher* principles.

It is expected that many courts may not be favourably disposed toward the adoption of such an argument. However, it is only through the innovative approaches of persuasive counsel that redress may be obtained for an otherwise dissatisfied plaintiff. Furthermore, every legal principle finds its origin or expansion in some innovative circumstance.

9. *Statutory Protection*

(a) *General Provisions*

Three of Canada's western provinces are seen as being in the forefront in the passage of privacy legislation.[90] Unfortunately, little if any progress has been made since the passage of this legislation. Two other provinces have followed the lead, but none of these provinces have updated their legislation to reflect changes in technology and the associated changing needs of our society.

One of the major criticisms of this legislation has been its lack of specificity. For instance, the lack of definition of privacy in the B.C. Act[91] makes the nature of the right being protected somewhat vague. The Manitoba and Saskatchewan Acts provide examples of violations[92] but do not provide any comprehensive definition of the right of privacy.

---

87. *Powell and Another* v. *Fall*, [1880] 5 Q.B.D. 597 (C.A.) at 601.
88. *Fingas* v. *Summerfeld Colony, supra,* note 86.
89. *Cf.*: *Dun & Bradstreet* v. *Greenmoss Builders, Inc., supra,* note 63.
90. *See* note 27, *supra.*
91. Atrens, "Comment on the Privacy Act", (1968) 26 Advocate 183.
92. Both in s. 3.

Additionally, the B.C. and Saskatchewan Acts both require wilful conduct[93] and the Manitoba Act requires substantial and unreasonable[94] behavior before an action may be brought.

All three of the Acts permit the bringing of an action without proof of damage.[95] The B.C. Act makes no reference to remedies. The Manitoba legislation enumerates a number of factors to be considered in awarding damages.[96] Presumably, this allows judicial discretion in determining the suitability of awarding punitive or exemplary damages and the possibility of mitigation of damages, due to the actual status or behavior of the plaintiff. The Saskatchewan Act leaves a fair degree of discretion to the court in awarding remedies.[97]

Two additional interesting points to be noted regarding these statutes are (a) the Saskatchewan Act specifically[98] binds the Crown, and (b) the Manitoba Act precludes the admission into evidence in a civil proceeding of any evidence obtained by virtue of a violation of privacy which could be actionable under the Act.[99]

In summary, it may be concluded that while these statutory provisions do provide a large measure of protection, which does not exist in other provinces, they are not readily amenable to the protection of the interests violated in our hypothetical examples (with the possible exemption of the deliberate violation of the taxation information).

In each instance, the legislation requires deliberate acts on the part of the violator. It is submitted that all of this legislation is directed at protecting a limited sphere of privacy and that it does not contemplate violations arising from careless or negligent behaviour. While it is wise to avoid legislation which opens the proverbial floodgates of litgation, it is important to recognize the need for additional safeguards for personal privacy.

To illustrate the limited protection afforded by such legislation, consider the case of *Davis* v. *McArthur*.[100] In this instance, the B.C. Court of Appeal overturned a lower court finding that the actions of a private investigator constituted a violation of the privacy of the complainant. Tysoe J., speaking for the court, indicated that such a right was "[subject to] the lawful interests of others"[101], and that:

---

93. R.S.B.C. 1979, c. 336, s. 1(1); R.S.S. 1978, c. P-24, s. 2.
94. S.M. 1970, c. 74, s. 2(1).
95. R.S.B.C. 1979, c. 336, s. 1(1); R.S.S. 1978, c. P-24, s. 2; S.M. 1970, c. 74, s. 2(2).
96. S.M. 1970, c. 74, s. 4(2).
97. R.S.S. 1978, c. P-24, s. 7.
98. *Id.*, s. 11.
99. S.M. 1970, c. 74, s. 7.
100. (1969), 10 D.L.R. (3d) 250; *rev'd* (1970), 17 D.L.R. (3d) 760 (B.C.C.A.).
101. (1970), 17 D.L.R. (3d) 760 at 764-5.

> . . . as the agent of the wife who had a legitimate interest in her husband's conduct . . . the appellant was not in breach of the provisions of the Privacy Act.[102]

No right is absolute; each is subject to limitations or qualifications. In this instance, the court chose to recognize a qualified right to intrude upon the privacy of the respondent. Without commenting on the merits of this particular case, it must be recognized that limits must be imposed upon all rights. The degree to which this is to be done, and who is to make that decision, are difficult yet important issues. If we do not want to have to resort to the courts every time one of these issues arises, we must have more clearly articulated principles. This does not have to imply more legislation, merely better legislation. If individuals are to govern their behavior in accordance with the law, they must have a reasonable opportunity of understanding what standards of behavior are expected. Later in this paper, it will be proposed that we may want to consider extending such rights to include protection against careless or negligent acts that lead to a compromise of the privacy of another individual.

(b) *Specific Provisions*

A general review of other legislation reveals a number of statutes, both federal and provincial, which make provision for the protection of what may be characterized as privacy interests. An exhaustive evaluation of such provisions will not be attempted here. Instead, a review of some of the provisions of representative statutes will be presented to demonstrate the nature and extent of the protection afforded by such laws.

i. *The Credit Reporting Agencies Act*[103]

This statute provides for the licencing and filing of a bond by all persons who intend to operate or act as a credit-reporting agency within the province of Saskatchewan. It defines files in a very broad context as:

> S. 2 (1)(d) . . . information about a consumer . . . regardless of how the information is stored

thereby catching paper, as well as microform or magnetic media storage as well as any new forms which may be developed (*i.e.*, laser or fiber-optic recording techniques).

Section 17 specifies that no agency will "knowingly divulge" the contents of files to other than a specified class of individuals and s. 19 requires that "reasonable steps" be taken to assure the maximum accuracy of information maintained. The consumer has a right under

---

102. *Id.*, at 765.
103. R.S.S. 1978, c. C-44.

s. 23 to know the contents of any file regarding him but is not entitled to be informed of the sources of any investigative information in that file. Additionally, under s. 25 a consumer has a right to challenge any information in the file and, where the agency refuses to delete it, to have attached to it, and any subsequent report, a statement setting forth the nature of the dispute respecting the information. This is the only remedy available to individuals under the Act. However, s. 30 provides for penalties by way of fines or imprisonment for violations of the Act.

ii. *Consumer Reporting Act, 1973*[104]

This Ontario statue is similar in form to the Saskatchewan Act except that it has a few additional provisions. Section 8(4) specifies that the files of a consumer reporting agency may not be sold, leased or the title transferred, except to a consumer-reporting agency registered under the Act. Section 11(1) ensures that consumers may access their files without charge, but s. 11(2) allows the agency to withhold, from the consumer, any medical information gained, with the consumer's consent, from a physician who has specifically requested, in writing, that it be withheld from the consumer in his own best interest.

Interestingly enough, the Act specifies, in s. 8(1), that operators and employees of agencies must not "knowingly" furnish any information from files to non-authorized recipients. However, s. 18(1), which deals with those persons employed in the administration of the Act, provides no such limitation. This potentially opens the door to an action in negligent disclosure,[105] providing such an action would be entertained by the courts. However, the likelihood of unwarranted disclosure is much greater with agencies than it is with government officials who administer the Act.

iii. *The Personal Investigations Act*[106]

S. 8(1) of this Manitoba statute limits a consumer's access to files to once every six months, unless he has been notified of a denial of some application for a benefit because of the contents of such a file. It also provides for the establishment of fees to be paid by the consumer for the inspection of his file. Sub-sections 11(2)and (3) provide for extra-territoriality by making the Manitoba resident liable for compliance with s. 11(1) of the Act where either the agency or the user of the information is non-resident. This sub-section relates to the verification of disputed information. In effect, whether a user or supplier of the information, the

104. S.O. 1973, c. 97.
105. S. 18(1) is a fairly strong argument for the recognition of a duty of care on the part of those individuals.
106. S.M. 1971, c. 23.

Manitoba resident bears the responsibility for verification when the other party is a non-resident.

Perhaps the strongest statement in relation to our concern with negligent disclosure is contained in s. 16, which states:

> No user, personal reporter or personal reporting agency is civilly liable to the subject of a personal report or personal file, unless the user, reporter or agency, as the case may be *is or ought to be reasonably aware* that part or all of the information in the report or personal file is false, or misleading, or was obtained negligently. [Emphasis added]

This is surely a classic definition of negligence and thereby affords an opportunity to advance an action, notwithstanding the prohibition on "knowingly divulging" information referred to elsewhere[107] in the Act.

iv. *Income Tax Act*[108]

Section 241 of the *Income Tax Act* includes several provisions regarding the communications of taxation information to non-authorized individuals. S. 241(1)(a) sets the standard of "knowingly communicating" or "knowingly allowing" the communication and thereby precludes the possible action for negligent disclosure if the *Income Tax Act* is to be used as a source of a duty which has been breached. Until 1981, only Revenue Canada staff or others defined as authorized individuals committed an offence; an individual receiving the information did not.[109] A change in 1981 created third party liability and thereby increased the level of protection afforded to the taxpayer.

As previously mentioned,[110] it has become apparent that there is no general policy on disclosure, and wide discretionary powers appear to be vested in the Minister and his officials. The department has invoked s. 241(2) on occasion to refuse to identify the address of an absconding husband who had taken his children after the court had awarded custody to the wife[111] or even denying release to the taxpayer of his own records.[112]

The Act does provide for fines and/or imprisonment for violation but civil remedies are limited to tortious actions against the specific individual(s) involved.

---

107. *Id.*, s. 5, s. 17(3).
108. R.S.C. 1952, c. 148.
109. *Id.*, s. 241 (9)(b).
110. See Laycraft's J. comments regarding the Royal American Shows inquiry, *supra,* note 20.
111. *Re Glover and Glover,* [1980] C.T.C. 531 (Ont. C.A.); *aff'd Glover* v. *M.N.R.,* [1981] 2 S.C.R. 561; 130 D.L.R. (3d) 383. More recent emphasis on maintenance order enforcement processes has seen the legislation of information exchange between government agencies.
112. *M.N.R.* v. *Die Plast Co.* (1952), 6 D.T.C. 1082 (Que. C.A.).

Given the secrecy which pervades the organization, and the refusal of departmental staff to identify themselves, even in general correspondence with taxpayers, it is highly unlikely that one who has suffered through an unauthorized disclosure of his tax information will find redress.

As a footnote to the foregoing, it is interesting to note the growing accessibility to federal tax records which is enjoyed by other federal and provincial governmental bodies. For example, it is not uncommon for other governmental agencies to tie the benefits of their programs to the tax status of individuals and corporations.[113] As part of the eligibility for such government benefits, the taxpayer is obliged to give a written authorization, to those agencies, which permits them access to the taxpayer's tax files held by Revenue Canada. As accessibility spreads and multiple copies of such information abounds, the likelihood of unwarranted disclosures of such information increases. Given the structure of the offences section (s. 241(a)) there is no application to individuals or organizations who receive this information directly from the taxpayer.

v. *Access to Information Act*[114]

This federal statute is not concerned with the protection of privacy, but rather with the granting of accessibility of information to the public. In principle, it potentially legislates the removal of privacy for the individual in regard to information held by federal government institutions. It does, however, provide[115] for the non-disclosure of personal information relating to individuals, subject only to the consent of the individual involved, the public availability of the information or the provisions of s. 8 of the *Privacy Act*.[116] In effect, this piece of legislation opens the door to availability of information but potentially places many hurdles in the path of those seeking access.

vi. *Privacy Act*[117]

This federal statute was enacted with the purported purpose of extending the protection of privacy currently enjoyed by Canadians. It must be remembered that it is limited in application solely to information which is held by federal government institutions.

---

113. *Eg.*, the Alberta Rental Investment Incentive Program.
114. S.C. 1980-81-82, c. 111, Schedule I (Section 1).
115. *Id.*, s. 19(1).
116. Discussed *infra.*
117. S.C. 1980-81-82, c. 111, Schedule II (Section 2).

It contains many commendable provisions, particularly those concerning the collection[118] and disposal[119] of information. For example, s. 4 specifies that:

> No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

S. 5 specifies that, wherever possible, information is to be collected from the individual to whom it relates, and the organization shall, except in specified circumstances, inform the individual that the information is being collected. The two specified circumstances are where compliance "might result in the collection of inaccurate information; or defeat the purpose or prejudice the use for which the information is collected". S. 6 imposes an obligation on the institution to ensure the accuracy of its information and addresses retention periods for the information being held. It also contains laudable provisions regarding periodic publication of indices[120] of files held by government institutions, as well as those concerning the complaint[121] and review[122] provisions involving the independent Privacy Commissioner. The powers of the Federal Court to review,[123] where access has been refused, and potentially order disclosure[124] or removal[125] of certain information are also spelled out.

These provisions are greatly overshadowed by some of the more questionable aspects of the Act. Notable among these are the fact that the only provision[126] regarding offences under the Act relates to obstruction of the Privacy Commissioner, and the fact that, although the Privacy Commissioner has the power to review all but very limited files,[127] he has no authority to order compliance. This office is limited to reviewing and reporting only. Government officials are free to ignore the recommendations of the Privacy Commissioner with impunity. Also questionable is the rather paternal nature of s. 28 relating to non-disclosure of medical information[128] and s. 8(2)(b) which appears to give politicians and senior

---

118. *Id.*, ss. 4-5.
119. *Id.*, s. 6.
120. *Id.*, s. 11.
121. *Id.*, s. 29.
122. *Id.*, s. 34-35.
123. *Id.*, s. 41.
124. *Id.*, s. 48.
125. *Id.*, s. 50.
126. *Id.*, s. 68.
127. *Id.*, s. 34(2).
128. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that relates to the physical or mental health of the individual who requested it where the examination of the information by the individual would be contrary to the best interests of the individual.

government officials the power to abrogate any protection afforded under this act.[129]

In conclusion, it would appear that, although there are significant statutory protections in existence, they are limited in scope and do not provide adequate coverage for the interests of the susceptible public. There can be no question that those provisions which do exist afford little or no safeguard in circumstances like those desribed previously in section III. Most of the legislation is limited to specific individuals, organizations or types of business and invariably, with only minor exceptions, they address themselves to deliberate acts of invasion or disclosure. Very little protection exists when we are dealing with the many organizations, not covered by such legislation, which collect and use large volumes of information concerning members of the public.[130]

V. *Control of Data Acquisition and Use*

Perhaps the greatest fear of those who are concerned with invasion of privacy is recognition of the fact that information supports power, and consequently, any concentration of power in the hands of data collectors could jeopardize the well being of the individual.

The question of regulation and control of computer-managed data bases has gained great prominence among those who have expressed concern about the potential threat posed to the privacy of the individual by these technological marvels. Proposals for achieving some measure of control have resulted in a diverse number of recommendations, each of which has its apparent strengths and weaknesses. It must be accepted, from the outset, that no single scheme or approach can hope to satisfy all the competing interests and thereby bring about a balance between the privacy of the individual and the legitimate needs of the data gatherers.

This section will review some of the most frequently identified proposals for controlling computerized information handling. Each will be discussed in terms of its approach and potential impact on the rights of individuals.

---

129. S.8(2). Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure.

130. With the possible exception of the general coverage offered by those provinces with privacy legislation or where a complainant can fit himself within the parameters of some specific tort action as described earlier in this section.

1. *Domestic Regulation*

The obvious answer to any requirement for control is the establishment of legislated rules governing activities or endeavors. Proposals and actual implementations in this area have covered a vast range of possibilities.

The most usual is the establishment of legislation covering specific industries such as those concerning credit-reporting agencies discussed in the previous section. This approach has varied to the extent that proposals have been advanced[131] for compulsory registration, and possibly licensing, of all systems which maintain personal data of any form.

Under the U.K. Data Protection Act,[132] a system of compulsory registration, guaranteed access and disclosure and formal review by a Data Registrar is to be applied to all "automatically" processed "personal" data. While the principle is commendable, one wonders if this proposal does not go too far. *Quaere* whether this would apply to normal business correspondence and, for that matter, legal documents not subject to privilege, prepared on a word processor in a law office, notwithstanding the appearance of exclusion of such information under s. 1(8) of the Act.

Perhaps the most comprehensive data protection legislation to be enacted to date is that of the Federal Republic of West Germany.[133] Under s. 41 of this Act, any person who communicates, modifies, receives or processes personal data, without authorization, is subject to the imposition of a fine or imprisonment. Harsher penalties attach (*i.e.*, two year maximum sentence) if the unlawful access was for financial gain. However, before any prosecution is undertaken, the citizen whose information has been violated must be aware of the violation and must complain to the authorities.

It has even been suggested that consideration be given to creation of a specific tort to regulate computer technology.[134]

2. *Control of Transborder Data Flow*

Considerable attention has been focused, in recent years, on the subject of transborder data flow. For the most part, any regulation or proposals

---

131. *See* "Proposed Pennsylvania Privacy Bill Could Create Data Bank Chaos", I Computer Law and Tax Report No. 1, Aug. 1974.

132. Royal Assent given 12 July 1984.

133. German Federal Data Protection Act of 1977 (*Bundesgesetzblatt*) [BGB1] I 201.

134. G. Kaiser, "Constitutional Aspects of the Regulation of Canadian Computer Technology" (1971), 1 Queen's L.J. 97. *See: Chatlos Systems Inc.*v. *National Cash Register Corp.*, 479 F. Supp 738 (D.N.J. 1979); and 635 F. 2d 1081 (3rd Circ. 1980) where an unsuccessful attempt was made to plead a new tort of computer malpractice.

to date have tended to be more concerned with the protection of domestic industry and the imposition of economic sanctions against non-residents[135] than with the protection of the privacy of individuals.

Even the guidelines of the Paris based O.E.C.D., concerning protection of individuals from the misuse of computer stored information, caution against the restriction of data flows across national borders.[136] Canada now subscribes to these guidelines.

While the establishment of international guidelines is a desirable goal,[137] it is feared that the persuasion of other member nations to open their borders to a free flow of data will provide a further erosion of our control over such information. It should be noted that there is a constant flow of personal credit-related information, on Canadian citizens, to the United States. The largest credit-reporting organizations are centered in the southeastern U.S.

3. *Licencing of Data Processing Personnel*

Other proposals have called for the mandatory licencing of those engaged in the data-processing field. This, in essence, represents a further extension of the licencing practices currently in use in the credit-reporting field. For such a scheme to be effective, it would necessitate the establishment of minimum qualifications and certification standards for personnel. This is something which the data-processing community has been unable to accomplish to date due to the sheer size and diversity of the field. It should be noted that advances are being made by industry associations, but participation is strictly voluntary on the part of individuals. This approach will ultimately improve the situation, but is not sufficient to meet the needs which exist.

4. *Industry Self-Regulation*

Very comprehensive proposals for self-regulation of the data-processing industry have been advanced.[138] If the experience of other professions such as law and medicine could be replicated in this regard, this could be part of the answer. However, due to the varied educational backgrounds and diverse roles of the individuals concerned, it is highly unlikely that

---

135. *See, e.g.,* R. Bigelow, "Transborder Data Flow Barriers" (1979), 20 Jurimetrics J. 8 and R. McGuire, "The Information Age: An Introduction to Transborder Data Flow", 20 Jurimetrics J. 1.

136. D. McMonagle, "Canada supports computer privacy", *Globe and Mail,* May 23, 1984.

137. The guidelines propose open export of information to those nations which comply with the guidelines, but not to others.

138. *See, eg.,* E. Grenier, Jr., "Computers and Privacy: A Proposal for Self-Regulation," [1970] Duke L.J. 495.

this would be possible. Data processors do not share a common bond as do lawyers and medical practitioners and they belong to a fairly young profession,[139] not having had the benefit of centuries of experience during which to establish themselves and appropriate principles and standards of behavior.

Attempts have been made, within the industry, to achieve certification of data-processing professionals,[140] but membership in industry associations is voluntary and those certifications which do exist are not universally recognized within the community.[141]

These organizations do represent a positive force in the advancement of the interests of the public through the development of guidelines such as those of the Council of the Association for Computing Machinery:

> 1.1 An A.C.M. member will have proper regard for the health, privacy, safety and general welfare of the public in the performance of his professional duties.
>
> 1.2 An A.C.M. member will act in professional matters as a faithful agent or trustee for each employer or client and will not disclose private information belonging to any present or former employer or client without his consent.

Unfortunately such statements tend to be "platitudinous"[142] and have little bearing on the behavior of the organizations' members. There is no monitoring and it is debatable whether members are even aware of the guidelines or code of behavior to which they subscribed when they joined the organization. At best, attempts at self-regulation can have only a slight measure of moral persuasion over the members of the profession.[143]

5. *Screening of Personnel*

It is a common practice for most governmental agencies, and some businesses, to do security clearances on staff who have access to confidential information and to require that they swear an oath of

---

139. Computers are still a fairly recent phenomenon having only been introduced during the early 1950s and not reaching any degree of widespread application until the late 1960s and early 1970s.

140. Most notably among these efforts are the certification offered to members of the British Computing Society (limited to British citizens) and the C.D.P. designation awarded upon successful completion of a comprehensive set of exams offered by the Institute for the Certification of Computer Professionals (I.C.C.P.).

141. They are generally sought by individuals who lack formal academic credentials within the field.

142. A. Miller, *The Assault on Privacy, supra,* note 61 at 255.

143. Unfortunately, like most occupational groups, industry associations are primarily concerned with advancing the interests of the profession.

secrecy.[144] However, with the spread of computer systems throughout the organization, more and more people are given access to greater volumes of information. It is doubtful that security and screening procedures have been modified to reflect the changing needs.[145] It is not uncommon to put full-time staff through rigorous screening yet give unsupervised access to cleaning staff or service people. Similarly, many organizations make frequent use of consultants and other contract resources yet do not screen those individuals. This increased accessibility by unchecked personnel contributes to a growing erosion of the limited control which does exist.

6. *Standards and Education*

Many of the problems which arise, and particularly those characterized in the examples of violations being addressed within this paper, are the result of the carelessness or inadvertence of the individuals involved. Two of the most effective means of dealing with these problems are the establishment of standards and the formulation of educational programmes to heighten the information processing profession's awareness of the problem.

While universal standards are desirable, it is unlikely that, short of legislated enactment, this will occur within the near future. It is therefore the responsibility of every organization which engages in the processing of personal information to set and maintain strict standards for the handling of that information. This may require some measure of internal policing to ensure that the established policies are being followed.

Considerable time and money is expended in post-secondary educational institutions and within the internal training programs of private and public sector organizations to prepare people for the new technologies. Almost all this training, particularly that aimed at the technocrats, is geared to the objective of getting the most out of the available technology. The emphasis which is given to concerns for security and privacy also tends to focus upon the technology and invariably pays short shrift to concerns for the privacy of the individual.

7. *Conclusion*

There is no doubt that changes to the methods and practices of the information handlers are necessary. But the question of how to best

---

144. The federal government goes further and fingerprints and does full security checks on individuals (employees and consultants) who may have access to such information.

145. While many organizations require their staff to swear an oath of secrecy, it is not unusual to give temporary or agency staff access to the same information with little or no precautions being taken.

achieve this result is difficult to answer. We are regulated enough in our lives that we can no longer afford to look to the passage of more regulations to handle every situation that arises. But do we really have a choice?

While the legal process affords some measure of protection, it is often slow, costly and retrospective in its application. Also, like striking a mule with a stick to get its attention, its effects are often soon forgotten or new ways of avoiding the sanction are discovered. Therefore, this approach must be seen as a means of redressing violations but not as a principal means of preventing such violations. Other approaches will no doubt be more suitable in achieving the desired result.

VI. *Proposals for Reform*

The general conclusion appears to be that the protection of privacy in Canada is at best sporadic. In the case of disclosure of computer-held data, and particularly in regard to careless or negligent disclosures, it is virtually non-existent.

The following proposals are offered as possible ways through which this situation may be alleviated:

1. Extension of the legislative recognition of a right of privacy throughout all Canadian provinces and territories;
2. Provision of a more clearly articulated definition of exactly what the right of privacy protects;[146]
3. Recognition of a standard (albeit a high standard to safeguard against vexatious actions) of negligence which would entitle individuals to redress;
4. Limitations on the use of data to the authorized purposes for which the data was originally obtained;[147]
5. Education of the public in regard to their right to withhold information[148] and their rights to privacy;

---

146. It is not necessary to enumerate the individual rights, but to define, in reasonably precise terms, the nature of the rights which warrant protection.

147. For an interesting discussion on the misuse of data for such purposes as mailing lists see Miller, *The Assault on Privacy, supra,* note 61 at 80-82.

148. Most people seem quite willing to divulge almost anything they are asked. It is through the availability of information such as someone's Social Insurance Number that the process of cross-matching of otherwise unrelated data becomes possible. The only legitimate uses of the S.I.N. are for the purposes of the administration of the Unemployment Insurance Plan and the Canada Pension Plan. An individual is within his rights to refuse to divulge this information to anyone else including other government agencies. Note: Revenue Canada is gradually adopting the S.I.N. as the prime identifier for personal income tax purposes notwithstanding that it was not originally intended to be used for this purpose. The *Income Tax Act* has been amended to incorporate the use of the S.I.N. as a legitimate purpose (s. 237).

6. Lessening the power of the collectors of information;[149]
7. Encouraging the establishment of comprehensive policies and standards to be adopted and applied by the data handlers;
8. Ensuring that mechanisms, which are employed, apply to all information, regardless of its form of storage.

Mandatory licencing and registration schemes do not ensure that privacy is protected. While this approach may be suitable to specific segments of the industry,[150] any attempt to adopt a blanket application to all information processing systems would create chaos. No legislated approach can solve the problem by itself.

By the same token, self-regulation, coupled with internal and industry standards, may not represent the ideal solution. They must, however, form a vital part of any overall scheme of information privacy in the highly computerized society in which we live.

VII. *Conclusion*

The refusal of Canadian courts to recognize the existence of a common law right of privacy has vastly limited the scope of protection available to individuals. The existence, in some provinces, of privacy legislation, coupled with other available remedies, has somewhat improved the avenues of redress. It is suggested, however, that this situation is far from desirable. The lack of consistency among jurisdictions and the limited protection offered by these schemes leave a large void within which the potential for abuse is significant.

There has been little movement in the Canadian common law in this area. One of the few exceptions is the case of *Motherwell* v. *Motherwell*,[151] in which the Alberta Court of Appeal affirmed the granting of an injunction against a woman who was harassing her father, brother and sister-in-law via telephone. In a very thorough assessment of the case, the court held that these acts constituted an invasion of privacy. The court did not go as far as to recognize this as a *sui generis* actionable matter. Instead, it held that this invasion was an extension of private nuisance.[152] Accordingly the judgment was based upon the recognition of the property rights of the plaintiff-respondents. In fact, the court, although allowing judgment to the sister-in-law in her own name, wrested with the

---

149. Due to the unequal bargaining power they hold, landlords, credit grantors, employers and even governmental agencies tend to request and receive, from the public, considerable information which is not essential to their purposes.
150. Such as the credit-reporting industry, discussed *supra*.
151. (1977), 1 A.R. 47; 73 D.L.R. (3d) 62 (C.A.).
152. (1977), 73 D.L.R. (3d) 62 at 67.

problem that the property in question was that of her husband. On this basis, it would appear that this judicial recognition of a right of privacy is quite limited in its future application.

With regard to the possible protection against negligent invasion of privacy, particularly through the misapplication of data-processing technology, we are a long way from realizing even a minimal level. This problem can only be overcome through the education of the public and potential violators to the inherent dangers associated with certain current practices. Without this awareness, the chances of success are quite limited.

Before we formulate new or changed methods of dealing with this situation it is important that we first assess one major factor — whether or not this is a right worthy of protection. If society's answer to this question is in the negative, then no further discussion is necessary. However, if we collectively respond positively, we are faced with further questions which must be answered, including the extent to which we are prepared to do so. From these starting points, it will be possible to formulate a comprehensive plan for the accomplishment of the identified objectives.

It must be noted, in closing, that protection against disclosure of confidential information is important in relation to information stored or handled in all forms. This paper has focused upon the use of computer systems in handling personal information. The reader must recognize that all the principles addressed within this paper should be equally applicable to all sources of information. It is submitted that the amendments to the *Criminal Code* (ss. 301.2 and 387), which created new offences, are too narrow. They should, in this writer's view, address all information, not only machine-processable information.