

1986

The Delicate Balance: Reconciling Privacy Protection With the Freedom of Information Principle

John D. McCamus

Osgoode Hall Law School of York University, jmccamus@osgoode.yorku.ca

Source Publication:

Government Information Quarterly. Volume 3, Issue 1 (1986), p. 49-61.

Follow this and additional works at: https://digitalcommons.osgoode.yorku.ca/scholarly_works



This work is licensed under a [Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Recommended Citation

McCamus, John D. "The Delicate Balance: Reconciling Privacy Protection With the Freedom of Information Principle." *Government Information Quarterly* 3.1 (1986): 49-61.

This Article is brought to you for free and open access by the Faculty Scholarship at Osgoode Digital Commons. It has been accepted for inclusion in Articles & Book Chapters by an authorized administrator of Osgoode Digital Commons.

The Delicate Balance: Reconciling Privacy Protection With the Freedom of Information Principle

JOHN D. McCAMUS

Many of the major western democracies have enacted freedom of information legislation in recent years. The author argues that these legislative schemes have not yet successfully resolved the tension between the desire for greater openness which these schemes manifest and a concern to protect personal privacy. The author compares the approaches taken in federal legislation in Canada and the U.S. and concludes that the former scheme permits undue sensitivity to privacy protection concerns to undermine the access scheme. The author concludes, however, that the American "balancing test," though preferable, could be much improved by the adoption of more specific criteria for achieving an appropriate balance, a number of which are articulated in this article.

In recent years, a number of the older democracies of the English-speaking world and of continental Europe have enacted freedom of information legislation. Developments in continental Europe have been very much influenced by the Swedish experience with access laws, stretching back over the past two centuries.¹ In the English-speaking countries, however, the major influence has undoubtedly been American experience with its federal Freedom of Information Act.² At the same time, public policy in these countries manifests an increasing sensitivity to the privacy protection issue.³ This article is concerned with the problem of legislative design thrown up by the apparent conflict between these disparate objectives of government information policy.

The freedom of information principle holds that, generally speaking, every citizen should have the right to obtain access to government records. The underlying rationales

John D. McCamus is Dean of the Osgoode Hall Law School, York University, Toronto, Ontario, Canada M3J 2R5.

most frequently offered in support of the principle are, first, that the right of access will heighten the accountability of government and its agencies to the electorate; second, that it will enable interested citizens to contribute more effectively to debate on important questions of public policy; and, third, that it will conduce to fairness in administrative decision-making processes affecting individuals.⁴

The protection of privacy principle, on the other hand, holds in part at least that individuals should, generally speaking, have some control over the use made by others, especially government agencies, of information concerning themselves. Thus, one of the cardinal principles of privacy protection is that personal information acquired for one purpose should not be used for another purpose without the consent of the individual to whom the information pertains. Absolute adherence to this principle is thought to be unworkable in practical terms and the principle is therefore typically hedged in by various exceptions in privacy protection legislation. Nonetheless, the principle represents the statement of an ideal from which the exceptions are taken. The philosophy underlying the privacy protection concern links personal autonomy to the control of data concerning oneself and suggests that the modern acceleration of personal data collection, especially by government agencies, carries with it a potential threat to a valued and fundamental aspect of our traditional freedoms.⁵

When attention is drawn to government records containing personal information concerning identifiable individuals, it is obvious that these two philosophies and legislation based upon them are capable of generating conflict. At the risk of belaboring the obvious, a few illustrations of the problem may be listed:

1. A journalist seeks access to government records that will reveal the salaries of the chief executive officers of all government-owned corporations.
2. A researcher doing a study of military justice seeks access to records of decisions in disciplinary matters.
3. A journalist, who believes that a particular agency has been lax in dealing with a particular problem, seeks access to records which reveal the actions taken by responsible officials.
4. A convicted offender, released from prison under supervision, commits an offence of violence. A journalist seeks access to letters written in support of the prisoner's release.
5. A journalist seeks access to government records which he believes will reveal that a public servant has engaged in improper financial dealings with public funds.

One could easily multiply examples of this kind. In each case, the individual seeking access wishes to scrutinize some aspect of the conduct of public business. In some cases, this will involve disclosure of information pertaining to public officials. In others, it will involve disclosure of information concerning ordinary citizens. In each instance, the subject of the information can plausibly raise a privacy protection concern. One man's freedom of information is another man's invasion of privacy.

This tension between the freedom of information and privacy protection principles creates essentially three policy problems for those who are engaged in designing

legislated freedom of information and privacy protection schemes. First, there arises the problem of institutional design. In what institutional forum should conflicts of this kind be resolved? In the courts? In the legislature? In the bureaucracy? Second, wherever these problems are to be addressed, what guidance can be given to those saddled with the resolution of such conflicts? This is the question of substantive policy. How, if at all, can these two conflicting values be reconciled? In this article, I address these two questions against the background of a comparative analysis of Canadian and American freedom of information and privacy protection statutes and the proposals of the Ontario Commission on Freedom of Information and Individual Privacy, which are set forth in the Commission's 1980 Report, *Public Government for Private People*, and which form the basis of a freedom of information bill recently introduced by the Government of Ontario.⁶

A third range of problems, essentially technical in nature, will not be addressed here. These problems arise from the potential for conflict between the general rights of access conferred by freedom of information laws and the more particular rights of access conferred by privacy protection laws which enable individuals to obtain access to information concerning themselves. It is no easy task to design access rights within these two different contexts which will co-exist harmoniously, and this has proven to be a continuing problem in the American federal experience.⁷ Suffice to say that in the Canadian context, these problems appear to have been for the most part resolved in the drafting of the federal Access to Information Act and the Privacy Act, as enacted in June of 1982.⁸

THE INSTITUTIONAL DESIGN PROBLEM: THE LOCUS OF CONFLICT RESOLUTION

Since conflict between the competing values of access to information and personal privacy appears inevitable, what is the ideal institutional location for the power to provide an authoritative resolution of these conflicts? The answer provided by the American federal legislation is that ultimate recourse is to be taken to the courts through judicial review of agency decisions to deny access. The U.S. Freedom of Information Act⁹ requires that federal government agencies make their records available to "any person" unless the records fall within one of nine exceptions of this general rule. The exception of relevance to the present discussion is that agencies may refuse to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."¹⁰ An individual who is denied access to a government record on the basis of the agency's conclusion that disclosure would be an unwarranted invasion of privacy, may challenge the agency's decision in the federal courts. The court will, in turn, reach its own conclusion as to whether or not the record is exempt from disclosure and, if satisfied that the public interest in access outweighs the individual data subject's interest in privacy, will order disclosure of the document in question.

The U.S. Privacy Act¹¹ is drafted to function consistently with the access scheme. Thus, although the Act generally prohibits disclosure of personal data without the consent of the data subject, there are some exceptions to this general rule and one of them permits disclosure under the Freedom of Information Act. Thus, the Freedom of

Information Act confers a right of access upon the requestor, the content of which is subject to judicial determination, and the Privacy Act confers a right of non-disclosure on the data subject, the content of which can again be tested in the courts. For the litigation-averse public servant, a premium is quite obviously placed on sound judgment. When confronted with a request for access to a record containing personal information, the agency confronts the twin possibilities that if it denies access it may be sued under the Freedom of Information Act whereas if it grants access, it may be sued under the Privacy Act. Nonetheless, the American scheme does provide an independent source of authoritative advice on the resolution of the tension between access and privacy values. It is not at all surprising that a sophisticated jurisprudence on this question is emerging in the American case law.¹²

Under the Canadian federal legislation, by way of contrast, reconciliation of the access and privacy values is left essentially to the discretion of public officials. Thus, although the Access to Information Act 14 confers a broad right of access to government records- a right which is for the most part subject to enforcement by the courts¹⁴-it exempts from this right access to records containing "personal information," this latter concept being very broadly defined indeed in the statute.¹⁵ This definition is itself subject to certain limited exceptions with the result that a very narrowly-conceived right of access to records containing personal information is contained in the Access to Information Act. As a general rule, however, access to such records is prohibited by the statute,¹⁶ although this prohibition is, in turn, made subject to whatever disclosures are permitted under Section 8 of the Privacy Act. The latter provision is the section of the Privacy Act which purports to control disclosure of personal information. Although it begins by stipulating that personal information shall not be disclosed without the consent of the individual data subject, it confers a series of discretionary powers on agencies to disclose information to a variety of individuals for a variety of purposes and concludes, in sub-section (m), that an agency has a discretion to disclose:

for any purpose where, in the opinion of the head of the institution,

- (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure, or
- (ii) disclosure would clearly benefit the individual to whom the information relates

The language of sub-paragraph (i) evinces a strong bias in favor of privacy protection, in contrast to the American provision which evinces strong support for the access principle, but this is a point to which we shall return in the next section of this article. The important point for present purposes is that, as far as personal information is concerned, essentially no right of access is conferred upon individuals seeking access and no right to control disclosure is conferred upon those who wish to prevent it. It is true that the two statutes both establish public officials, the Information Commissioner and the Privacy Commissioner respectively, whose mandates include a duty to entertain complaints concerning proposed withholdings or disclosures under either statute. However, the Commissioners possess only the powers of an ombudsman-that is, they can make recommendations but cannot compel an agency to withhold or disclose.

In sharp contrast to the American scheme, then, the Canadian statute addresses the problem of resolving the conflict between access and privacy by simply suppressing it into the level of administrative discretion and refusing to confer rights of access and rights to prevent improper disclosure.

In adopting this approach, the Canadian scheme has, in my view, both substantially undermined the access rights conferred by the Access to Information Act and significantly depreciated the degree of privacy protection afforded by the Privacy Act. As far as the access right is concerned, it should be emphasized that a very substantial percentage of government records must contain information pertaining to identifiable individuals which would bring them within the sweep of the far-reaching definition of personal information contained in these statutes. To confer so broad a discretion on the federal bureaucracy to withhold or disclose such information is to simply ignore the basic premise of freedom of information legislation, i.e., the conferral of a *right* of access on the public at large.

If it is the point of the federal Canadian scheme to sacrifice freedom of information in order to effect a high level of privacy protection, then it must be said that the federal bureaucracy is also not the most suitable instrument for the achievement of this objective. Public officials are placed in a position of conflict of interest when asked to disclose information which might facilitate effective public scrutiny of their performance. It may well be in the interests of a particular department to disclose information and demonstrate that it has conducted public affairs in a perfectly sound and responsible fashion, notwithstanding the substantial invasion of the privacy of identifiable individuals which may result from disclosure.

A leading American decision under the Freedom of Information Act illustrates the problem. In *Sonderegger v. United States Department of the Interior*,¹⁷ certain journalists sought access to claims files arising in the context of special federal assistance programs for the victims of a flood which had devastated a town in Idaho. The journalists obviously wished to detect malfeasance in the handling of such claims and the federal agency was quite willing to permit full disclosure. The flood victims, on the other hand, felt that disclosure would substantially invade their privacy, inasmuch as each claim represented essentially the net worth of the individual in question. As well, they felt that disclosure would prove to be very stressful for a community which was already enduring considerable stress in attempting to re-establish itself after this disaster. Expert evidence was provided by a psychologist who was working with the local committee, confirming this prognostication. The federal court decided that the public interest in disclosure was significantly outweighed by the resulting invasion of the privacy of the plaintiff townspeople and, thus, overruled the decision of the agency to permit disclosure. One can understand that public officials are anxious to dispel unfair allegations of wrongdoing. My point simply is that there will be situations in which the question of disclosure cannot be approached in a completely disinterested fashion. The enactment of a freedom of information statute represents an acknowledgement of this plain fact and the adoption of a remedy which places the decision to disclose the document effectively beyond the powers of the officials concerned.

A substantial problem with the Canadian scheme, then, is that it establishes a far-reaching domain of discretionary power which, at one and the same time, creates the risk that access to records will be denied in order to preclude appropriate scrutiny of public

affairs on the pretext that disclosure will unfairly invade the privacy of data subjects and, on the other hand, the risk that public officials concerned to clear their good names will be tempted to do so, notwithstanding the fact that disclosure will affect a substantial invasion of the personal privacy of individuals.

A further problem with the Canadian scheme is that it conduces to a wilderness of inconsistent decision-making from one department and governmental unit to the next. One finds little or no guidance in the statute itself as to how the discretion to disclose should be exercised. More surprisingly, perhaps neither does one find assistance in the Treasury Board's Interim Policy Guide which sets forth extensive guidance for public officials on the proper interpretation and implementation of other aspects of the Access to Information Act and the Privacy Act.

A more sympathetic observer of the Canadian scheme might argue that the problem is, after all, an intractable one and suggest that the legislation in its current form will at least provide a splendid opportunity for the Information Commissioner and the Privacy Commissioner to investigate matters of this kind and assist the bureaucracy in developing helpful guidelines for resolving conflicts of this kind. It is difficult to discern, however, that either Commissioner will have a substantial role in dealing with this issue. As far as the Information Commissioner is concerned, if the information in question clearly falls within the definition of personal information, and surely this will often be so, there does not appear to be much for her to say, other than that the record in question is, indeed, exempt from the access scheme. As far as the Privacy Commissioner is concerned, provided that the public official in question has, in good faith, weighed the public interest in disclosure against the privacy value, it is again difficult to see that much remains to be said by the Commissioner. It may well be, however, that given the importance of this question and the absence of any other source of guidance, either or both Commissioners will see fit to comment either on the inadequacies of the current legislative scheme or on the deficient exercise of the discretion which is unquestionably conferred upon public officials by it.

Two explanations may be offered for the Canadian reluctance to extend judicial review into the area of records containing personal data. First, it may be felt that this is an attempt to avoid burdening data subjects with either the cost or the inconvenience of participation in judicial review. Second, it may be thought that so important a question as this ought not be simply remitted to the courts.

With respect to the first point, a preferable solution would have been to endow the Privacy Commissioner with the power to bear the cost of litigation of this kind on behalf of the data subject. One of the great innovations of the Access to Information and Privacy Acts was to confer a power of this kind on both the Information Commissioner and the Privacy Commissioner in the context of access requests. Where either Commissioner believes that the information should be made available over the objection of the governmental institution in question, the Commissioner is entitled to carry litigation brought on behalf of the requester and thus provide an authoritative resolution of the dispute which is cost free to the requester.¹⁸ The Privacy Commissioner could have been similarly empowered to provide cost-free litigious protection to the data subject.

With respect to the appropriateness of the courts as the instrumentality for resolving these conflicts, it would appear that the only other alternative to the bureaucracy itself would be the legislative branch of government. Indeed, many statutes which establish

administrative mechanisms requiring the collection of personal data do explicitly provide for the protection of the data. While the notion of resort to the legislature has an obvious democratic appeal in this context, two reservations about the capacity of the legislature in a parliamentary system of government to deal effectively with these issues must be registered. First, a legislature dominated by a majority party is easily seen to be subject to a version of the same conflict of interest that plagues the executive branch. The Access to Information Act notwithstanding, a Canadian government is not likely to vigorously pursue a policy of drafting legislation to ensure effective scrutiny of its own conduct of public affairs. Second, it should be noted that many legislative provisions of this kind are currently to be found in the statute book and, consistently with the hypothesis just stated, they typically provide that there is to be no access whatsoever to the data in question. The concern that such provisions may conduce to too much secrecy is manifested in Section 24 of the Access to Information Act, which requires that all such provisions be reviewed by a Parliamentary Committee within three years of the enactment of the Access to Information Act. Accepting, as I do, that provisions of this kind relating to personal data were often enacted purely for privacy protection purposes, they are typically drafted without any apparent sensitivity to the desirability of permitting some forms of access to even reasonably sensitive data. Thus, as David Flaherty demonstrated in a paper prepared for the Ontario Commission, much useful medical research has been thwarted by the existence of provisions of this kind.¹⁹ Leaving these reservations aside, however, it nonetheless is true that one possible response to the concern that the courts should not be given too much discretion in matters of this kind would be to specifically enact access and disclosure schemes to deal with specific information contexts.

As a more general matter, however, there are a number of difficulties inherent in the current Canadian model of administrative discretion and in a general referral to the legislature. This, together with what appears to be reasonably positive American experience, suggests that judicial review is the most attractive of the alternatives. The Ontario proposals and the recently introduced Ontario bill, attempt to improve on the U.S. scheme by providing for a binding determination by an independent administrative tribunal prior to ultimate recourse to judicial review.²⁰ Whether the reconciliation of privacy and access principles is to be located in the legislature or in the courts or the bureaucracy, or perhaps all three, the difficult question that remains, and to which we now turn, is how one should approach the task of effecting that reconciliation in analytical terms.

THE SUBSTANTIVE PROBLEM: ACHIEVING AN APPROPRIATE BALANCE

Again, the American and Canadian models provide interesting points of contrast. As has been indicated, the American statute provides a right of access unless disclosure of personal data would constitute a "clearly unwarranted invasion of privacy." The Canadian statute, on the other hand, provides for essentially no right of access, but for the right to obtain documents containing information in three categories:

1. Certain basic information concerning the contracts of employment of public servants and their opinions or views given in the course of employment;

2. Similar information concerning individuals performing services for a government institution under contract; and
3. Information "relating to any discretionary benefit of a financial nature, including the granting of a licence or permit."²¹

Presumably, the draftsmen of the Canadian statute thought that a more precise provision of this kind had some advantages over the vague standard of the American "clearly unwarranted invasion of privacy" test. Nonetheless, the difficulties created by a refusal to embrace a balancing test of some kind are manifest in this provision. As an access right, the Canadian provision leaves much to be desired. The illustrations with which I began this article were carefully chosen with this point in mind. They are all situations in which, in my view, a strong claim for access can be made and they are all situations in which access would be granted under the American scheme, notwithstanding the fact that all involve disclosure of personal information.²² They are also all situations in which no access would be given as right under the Canadian statute.

From the privacy protection point of view, the Canadian provision is also flawed. Although one understands the obvious rationale for requiring disclosure of information relating to discretionary benefits, such as licences, it should be noted that most welfare schemes, perhaps all such schemes, contain modest discretionary features. Thus, whether we speak of unemployment insurance benefits or widows' benefits under veterans' assistance legislation, or the various forms of assistance rendered to those suffering from mental or physical disabilities, some financial benefits typically remain within a discretionary category. There appears to be no merit whatsoever in conferring, as the Canadian statute does, a right of access to personal data pertaining to discretionary benefits of this particular kind.

A strong case can be made, then, for the desirability of a balancing test of some kind. Indeed, this is accepted in the Canadian statute to the extent that apart from the limited right of access to personal data conferred in the Access to Information Act, all other disclosures are to be made—though purely as a matter of administrative discretion—on the basis of a balancing test. The question that remains to be considered is how this balancing test should ideally be designed. Before offering some suggestions to this end, two preliminary points can usefully be addressed.

First it should be noted that to some extent the conflict between freedom of information and privacy protection can be resolved by deleting the names of identifiable individuals before releasing the requested documents. Anonymous data of this kind will often meet the needs of the requester and retard, if not completely eliminate, the risk of privacy invasion. As the leading U.S. case of *U.S. Department of the Air Force v. Rose*²³ indicates, however, even where some risk of identification or privacy invasion remains, deletion of names may take the task of balancing the public interest in access against the risk of privacy invasion an easier one. In *Rose*, legal researchers engaged in a study of military discipline sought access to records relating to Air Force disciplinary proceedings. They conceded that access to records with names deleted would be sufficient for their purpose but it was objected by the defendant that even with names deleted, it would be possible in many instances for individuals who were familiar with the incidents in question to identify the person disciplined. The federal court held that although this risk

was present, it was outweighed in the present case by the public interest in the ability of outsiders to scrutinize this area of government activity.

In any case where the deletion of names or other identifying detail prevents the identification of individuals, the requester should be able to rely upon the principle of severability, i.e., the principle embraced by both the American and Canadian access statutes that the government must disclose any reasonably severable portion of a requested document that is not covered by one of the exemptions.²⁴ One of the lessons of the *Rose* case, however, is that even where the elimination of identifiability cannot be achieved in this way, one may nonetheless reduce the risk of privacy invasion to the point where it is outweighed by the public interest in access.

A second point which has surfaced in the American case law applying the "clearly unwarranted invasion of privacy" test is whether the specific use of the personal data proposed by the requester is to be relied upon as the basis for testing the public interest in disclosure. Thus, where the requester has some highly beneficial medical or other research in mind, is it the potential benefit of such research that should be weighed against the invasion of privacy or, inasmuch as disclosure is likely to mean that the personal data can have a wider circulation in the public domain, should the particular use of the requester be ignored? In the U.S. experience and literature, discussion of this issue has been provoked by the decision in *Getman v. NLRB*,²⁵ a case in which certain law professors specializing in labor relations were allowed access to lists of employees eligible to vote in union representation elections in order to carry out research on certain policies of the U.S. National Labor Relations Board relating to the certification process. The court in *Getman* awarded access to the requesters specifically for the purpose of this project, and on the faith of an undertaking by them that they would not disclose the names of the individuals to anyone else. It is not at all evident that the disclosure of these names to the public at large would be sustained. Indeed, given the apparent absence of any public benefit from such disclosure, this would likely be characterized as an unwarranted invasion of personal privacy-hence the *Getman* court's concern that the requesters make no further disclosure of the employee lists. In *Getman*, then, the Court was prepared to grant limited access to the particular requester, even though access to the public at large would be inappropriate.

The debate stimulated by *Getman* has been rather intense.²⁶ Some have objected to the decision on the grounds that inasmuch as the Freedom of Information Act provides access to "any person," the particular requester's "need to know" ought to be considered irrelevant. Others have given a policy justification for this reading of the statute which, to my mind at least, is compelling. If one does embrace a "need to know" concept in some of this case law, it is likely to spread its influence throughout the case law dealing with the conflict between freedom of information and privacy protection and very substantially undermine the value of the access right. Moreover, it seems impractical to contemplate a general practice of trying to restrain further disclosures of information released to requesters under the Freedom of Information Act. A far better solution, it seems to me, and one that was in fact proposed in the report of the Ontario Commission, and adopted in the recent Ontario bill is to treat the problem of access for research purposes as a separate problem and to devise a mechanism for providing access to personal data for the research community.²⁷

Turning then to the central question, how is one to strike a balance between freedom of information and privacy protection, the question essentially is whether one can do any

more by way of providing guidance to decision-makers than to offer the general instruction provided, albeit in significantly different terms, by both the American and Canadian statutes that the decision-maker should carefully weigh the public interest in disclosure against the personal interest in privacy protection. My own view is that one can substantially improve on this approach by attempting to articulate a variety of more explicit factors that should be taken into account by someone undertaking the task of reconciling these two interests. The following propositions derive, in the main, from discussion set forth in the Ontario Report²⁸ to the same general effect and from a reading of the American case law applying the "clearly unwarranted invasion of privacy" test.

I would suggest that the following factors should be considered pertinent in attempting to balance these conflicting interests:

- A. Is access to the information necessary to enable an individual to accomplish any of the objectives underlying freedom of information legislation, i.e., effective scrutiny of the activity of government institutions, effective participation in discussion concerning public affairs and increased fairness in administrative decision-making affecting individuals?

As I have already indicated, it may be asking too much of human nature to allow public officials themselves to determine whether a particular request is well suited to accomplish these objectives. The issues raised by these criteria for access are not particularly subtle, however, and could be answered with some confidence by third parties in most instances.

- B. Is access to the information in question likely to make a positive contribution to the promotion of public health or safety?

In addition to the generally accepted political rationales articulated in point (A), the granting of access to information with health and safety objectives in view appears to be accepted as a desirable spinoff of freedom of information legislation. Requests put forward for these reasons offer a particularly compelling interest in access.

- C. Will access to the information in question promote an informed choice in the purchase of goods and services?

Again, this appears to be a desirable incidental spinoff of freedom of information schemes. It is of no little interest that items (B) and (C) both find some philosophical support in Section 20 of the Canadian Access to Information Act which explicitly provides for access to the results of product and environmental testing and, more generally, confers upon government institutions a discretion to disclose commercial information if the public interest in public health, public safety or protection of the environment outweighs the harm that might result to the commercial party to whom the information pertains.

- D. Will the granting of access have the effect of benefiting the individual who is the subject of the information disclosed?

There may well be situations where the individual seeking access has only in mind the conferral of some benefit on the data subject and the case for disclosure in such circum-

stances is obviously compelling. This consideration is explicitly set forth in Section 8(m) of the Privacy Act as a basis for exercising the discretion to disclose.

E. Is the information of a kind which is normally disclosed in other contexts?

The fourth illustration set forth at the beginning of this article asked whether letters written in support of the release of a prisoner should be available to the public. These were the facts of a decision under the American Act, *Philadelphia Newspapers Inc. v. U.S. Department of Justice*,²⁹ in which the court reasoned that inasmuch as such individuals are acting, in a sense, as character witnesses for the convicted person, something they would normally be required to do in a public hearing, their letters should be made available. Here, as elsewhere in legal analysis, fruitful analogy is an important source of guidance.

A number of factors may be taken to weigh in the balance against disclosure:

F. Will access to the information frustrate the objectives of the statutory scheme under which the information was originally collected?

There may well be situations, for example, where conciliation procedures are mandated by a statute, where a disclosure of records will render the governmental institution in question effectively unable to carry out its assigned statutory task. Surely this would weigh heavily against disclosure.

G. Is the personal information of an especially sensitive kind?

It is possible to identify types of information such as medical information or information relating to eligibility for social service or welfare benefits, the disclosure of which would be seen by the average data subject as an especially grievous invasion of privacy.³⁰

H. Is the information unlikely to be accurate or reliable?

The probability that personal data will be accurate may vary quite considerably with the circumstances under which it is gathered or submitted, and the safeguards established or verification procedures adopted by the government institution in question. The likelihood of circulating inaccurate information should weigh against a decision to disclose.

I. Is there some prospect that the data subject will suffer substantial harm, pecuniary or otherwise, as a result of the disclosure?

Some invasions of privacy may serve not only to embarrass or otherwise diminish the sense of privacy of the individual data subject, but also cause substantial harm of one sort or another. This, again, should weigh against disclosure.

J. Was the information submitted on the basis of an expectation, tacit or otherwise, that it would be treated in a confidential fashion?

American courts have suggested that, although an undertaking of confidentiality should weigh heavily against disclosure, it should merely be a factor taken into account in deter-

mining whether or not to make the information available.³¹ Presumably such undertakings would normally be adhered to but perhaps not, for example, where the individual who initially supplied the information did not rely on the undertaking in any meaningful sense or was in any event by law to submit the information in question.

No doubt intimate experience with the functioning of freedom of information and privacy protection schemes would enable one to offer further propositions of this kind.

The Ontario Commission recommended a rather elaborate statutory provision³² in which a number of the foregoing propositions were stated as presumptions to be employed in the application of the balancing test and, I confess, I remain convinced that this is an attractive solution to the problem presented in this article. The Ontario bill contains a slightly revised version of this provision.³³ At the very least, however, it seems to me that the articulation of principles of this kind should be of assistance to those charged with the task of applying the more vague standards set forth in the American and Canadian legislation.

Privacy is an important but surely not an absolute value, and one which must compete with other values such as the public interest in access to government information. There is a serious danger that the concern to protect privacy will be allowed to submerge the access value, as the virtually wholesale exclusion of personal information from the Canadian Access to Information Act amply demonstrates. It is not too much to suggest that undue deference to the privacy value has substantially undermined the value of the Canadian access scheme. In remitting the question of whether to disclose personal information to the realm of discretionary power, the draftsmen of the Canadian scheme shied away from the task of reconciling these conflicting values. The Ontario bill, on the other hand, may be thought to represent a substantial improvement on the American experience. In this, and in other respects, the Ontario bill is a pioneering effort, worthy of serious attention by all who take an interest in freedom of information and privacy protection issues.

ACKNOWLEDGMENT

An earlier version of this article was read at a conference held in Toronto, Canada, on May 22, 1984 and published as part of the conference proceedings (see R. Wall, ed., *Conference on Privacy: Initiatives for 1984* (Provincial Secretariat for Resources Development, Toronto, Ontario, Canada, 1984, p. 51).

NOTES AND REFERENCES

1. See, generally, D.C. Rowat (ed.), *Administrative Secrecy in Developed Countries* (New York: Columbia University Press, 1979), and S.V. Anderson, "Public Access to Government Files in Sweden," *American Journal of Comparative Law*, 21(1973):119.
2. 5 U.S.C. Sec. 552. Freedom of information legislation has been recently enacted in New Zealand and, at the federal level, in Australia and Canada. In Canada, provincial access schemes have been enacted in New Brunswick, Newfoundland, Nova Scotia, Prince Edward Island, and Quebec. Recently government bills have been introduced in Manitoba and Ontario. The United Kingdom remains sturdily immune from these developments. See, generally, J. Michael, *The Politics of Secrecy* (Harmondsworth, U.K.: Penguin, 1982).
3. The literature on privacy protection is now voluminous. For a recent and extensive international

- bibliography, see D.H. Flaherty, ed., *Privacy and Data Protection: An International Bibliography* (White Plains, N.Y.: Knowledge Industry Publications, 1984).
4. See Ontario Commission on Freedom of Information and Individual Privacy, Final Report: *Public Government for Private People*, Vol. 2 (1980) (hereafter, *Ontario Report*), pp. 77-81; J.D. McCamus, ed., *Freedom of Information: Canadian Perspectives* (Toronto: Butterworths, 1981).
 5. *Ontario Report*, vol. 3, pp. 495-515. See, generally, A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967); James B. Rule et al., *The Politics of Privacy* (New York: New American Library, 1980).
 6. Ontario Legislative Assembly, First Session, 33rd Legislature, Freedom of Information and Protection of Privacy Act, 1985, (introduced for first reading, July 12, 1985) (hereafter, the Ontario Bill).
 7. See, *Ontario Report*, vol. 3, pp. 789-798.
 8. Canada, Parliament, First Session, 32nd Parliament, 1980, House of Commons, Bill C-43 (an Act to Enact the Access to Information Act and the Privacy Act, to amend the Federal Court Act and the Canada Evidence Act, and to amend certain other Acts in consequence thereof) as passed by the House of Commons, June 28, 1982 (hereafter the Access to Information Act or the Privacy Act). See, generally, T.M. Rankin, *The New Access to /reformation Act: A Critical Annotation* (1983), 15 *Ottawa Law Review* 1.
 9. 5 U.S.C. Sec. 552.
 10. *Ibid.*, (b)6.
 11. 5 U.S.C. Section 552a.
 12. See, generally, James T. O'Reilly, *Federal /reformation Disclosure*, vol. 2 (Colorado Springs, Col.: McGraw-Hill, 1983), pp. 1-38, c. 16.
 13. Access to Information Act, Sec. 4 (l).
 14. *Ibid.*, Sec. 41.
 15. Privacy Act, Sec. 3.
 16. Access to Information Act, Sec. 19.
 17. 424 F. Supp. 847 (1976).
 18. Access to Information Act, Sec. 42; Privacy Act, Sec. 42.
 19. D.H. Flaherty, *Research and Statistical Uses of Ontario Government Personal Data*, Ontario Commission on Freedom of Information and Individual Privacy Research Publication 5 (Toronto: Government of Ontario, 1979).
 20. See, *Ontario Report*, vol. 2, pp. 356-363; Ontario Bill, Sec. 46.
 21. Privacy Act, Sec. 3, (j) to (l) of the definition of personal information."
 22. Cases 2 and 4 are the most problematic. For authorities allowing access, respectively, see *U.S. Department of the Air Force v. Rose*, 424 U.S. 352 (1976); *Philadelphia Newspapers Inc. v. U.S. Department of Justice* 405 F. 2d 670 (DC Cir 1971). In *Rose*, the requestor sought access to the files with names deleted but the granting of access still offered the prospect of some privacy invasion as readers familiar with the incidents in question would be able to link the files to named individuals.
 23. 425 U.S. 352 (1976).
 24. Access to Information Act, Sec. 25.
 25. 450 F. 2d 670 (DC Cir 1971); cf. *Masonic Homes v. NLRB* 550 F. 2d 214 (3d Cir 1977)(employer denied access to union cards signed by its own employees). See also, *National Association of Atomic Veterans Inc. v. Director of Defence Nuclear Agency* 583 F. Supp. 1483 (DCDC; 1984).
 26. See, generally, F.A. Rosenfield, *The Freedom of/reformation Act's Privacy Exemption and the Privacy Act of 1974 [1976]*, 11 Harv. Civ. Rts. — *Civil liberties Law Review* 596 vat 611-618; A.T. Kronman, *The Privacy Exemption to the Freedom of Information Act [1980]*, 9 *Journal of Legal Studies* 727 at 767-770.
 27. *Ontario Report*, vol. 2, pp. 332-337; Ontario Bill, Sec. 21(l)(e).
 28. *Ibid.*, vol. 2, pp. 324-338.
 29. 405 F. Supp. 8 (ED Pa 1975).
 30. For an attempt at a more elaborate list of such information, see, *Ontario Report*, vol. 2, p. 338.
 31. *Robles v. EPA*, 484 F. 2d843 (4th Cir 1973); *Washington Post Co. v. U.S. Dept. of Health and Human Services*, 690 F. 2d 252 (CADC 1982).
 32. *Ontario Report*, vol. 2, pp. 335-338.
 33. Ontario Bill, Sec. 21.