

enforcement investigations cannot be availed of unless there is a prospect of proceedings. Thus the US equivalent was interpreted as not being intended to 'endlessly protect material simply because it [is] an investigatory file'.¹⁸ This approach has been confirmed in Australia.¹⁹

The Court went on to say that when such an exception is invoked by the Commission, it is obliged to indicate:

at the very least by reference to categories of documents, the reasons for which it considers that the documents detailed in the request which it received are related to the possible opening of an infringement procedure. It should indicate to which subject matter the documents relate and particularly whether they involve inspections or investigations relating to a possible proceedings for infringement of community law.²⁰

The Commission was found to have failed to have met this requirement.

With respect to the confidentiality exception, the approach adopted in *Carvel* was followed and it was held that the Commission must exercise its discretion by striking a genuine balance between, on the one hand, the interest of the citizen in obtaining access to those documents and, on the other, its own interest in protecting the confidentiality of its deliberations. The Court found there was no evidence that the Commission had fulfilled its obligations in this regard.

The decision to refuse access was annulled. The practical effect of the decision is that the Commission can choose either to appeal the case to the Court of Justice, or to release the documents or it can adopt a more satisfactory justification for the refusal.

The extent to which these decisions have helped to explain the meaning of the exceptions to the Code and Council decision is debatable. They have tended to focus more on the manner in which the exceptions are to be applied than on the substantive claim for exemption, and in so doing have set important standards for the exercise of the exception provisions. However, the value of the decisions from the standpoint of assessing the circumstances in which exceptions to the right of access will be permitted, is not so apparent. In the *Carvel* case the substantive issue was not addressed at all since the court disposed of the matter on a procedural point. In the *WWF* case the only substantive matter dealt with, namely the refusal of access to documents on the basis that they related to investigations which may lead to an infringement procedure, was addressed in a restrictive manner. There is still plenty of scope for the development of a jurisprudence concerning the interpretation of the exceptions in the Code and Council decision.

MAEVE McDONAGH

Maeve McDonagh teaches law at the University of Cork, Ireland.

References

1. 'A Government of Renewal: A Policy Agreement between Fine Gael, the Labour Party and Democratic Left', December 1994, p.7.
2. See McDonagh, M., 'Freedom of Information Proposals in the Republic of Ireland', (1996) 62 *Fol Review* 14.
3. Minister of State Eithne Fitzgerald.
4. The most active proponents of the introduction of Freedom of Information legislation in the UK is the Campaign for Freedom of Information, Director: Maurice Frankel, which was founded in 1984.
5. Private members Bills have been introduced by MPs Clement Freud (1978), Frank Hooley (1981), David Steel (1984), and Archie Kirkwood (1992).
6. For a detailed discussion of the Bill see Birkinshaw, P., *Freedom of Information: the Law, the Practice and the Ideal*, Butterworths, 1996, pp.336-348.
7. Council Directive 90/313/EEC on Freedom of Access to Information on the Environment.
8. 1993, HMSO Cm 2290.
9. From April 1994, when the Code came into force, and December 1996, 119 complaints about access to information were received. Of these, 66 were not suitable for investigation mostly for lack of evidence. In the 26 investigations complete up to 30 January 1997, the complaint was upheld or partly upheld in 17 cases and found not to be justified in nine cases.
10. Frankel, M., 'State's Open Secrets: How Effective has the New Code Been in Making Government More Transparent', *Guardian*, 24 January 1995.
11. In a third case a challenge by the Netherlands Government to the legal basis of the Code of Conduct and Council decision on access was rejected by the Court of Justice: *The Netherlands v EC Council* [1996] 2 CMLR 996.
12. See further McDonagh, M., 'Freedom of Information Developments in Europe', (1995) 58 *Fol Review* 59.
13. This Court has first instance jurisdiction in certain forms of action and appeals lie from its decision to the Court of Justice on points of law.
14. *Carvel & Guardian Newspapers v EU Council* [1995] 3 CMLR 359.
15. At 372.
16. *WWF UK (World Wide Fund for Nature) v Commission of the European Communities*, Case T-105/95, Judgment of the Court of First Instance, 5 March 1997, not yet reported.
17. At 15, transcript.
18. *NLRB v Robbins Tire & Rubber Co.*, 437 US at 232.
19. *Edelsten v Australian Federal Police* (1985) 9 ALN 65, D140.
20. At 17, transcript.

Secrecy: Report of the United States Commission on Protecting and Reducing Government Secrecy

On the 3 March 1997 the Moynihan Commission, more formally known as the Commission on Protecting and Reducing Government Secrecy, delivered its report to the President and Congress of the United States. While its report dealt with 'an investigation into all matters in any way related to any legislation, executive order, regulation, practice, or procedure relating to classified information or granting security clearances', its findings and analysis

have some lessons for the future direction of freedom of information in Australia.

Trends in Australian access law, including the increasing resort to the shibboleth of 'commercial in confidence' and wider developments like contracting out and privatisation necessitate changes in our conceptions of accessing information. When Jim Spigalman penned his book *Secrecy: Political Censorship in Australia* in 1972, free

dom of information was seen as a key device in accessing information vital to the democratic process. At that time the information was warehoused in one location — the public sector — and under one generic label — government information — and thus freedom of information legislation was designed to deal with this unsophisticated handling of democratic information. In the late 1990s that information has been relocated to a multitude of storage sites, repackaged under a plethora of labels and often forcefully removed from its democratic antecedents.

In rethinking our approaches to access we need to search for new frames of analysis that allow us to balance competing uses for that information. In terms of the Moynihan Commission focus, i.e. the classification of security information, are there ways of classifying and handling information so that security considerations are satisfied but as well the vast bulk of information is available for public use, discussion and to serve accountability functions?

The Moynihan Commission has suggested a number of mechanisms that if recast for Australian freedom of information regimes could allow us to move to a higher level of information analysis beyond the artificial and arid exchanges of 'this is commercial in confidence' to 'no it is not or if it is, the public interest demands its release'. At the moment Australian freedom of information management only requires thought to be seriously given to the classification of information on the haphazard receipt of a particular FoI request. The life cycle of information is only an oblique consideration that is occasionally called up in applying public interest tests.

This article outlines some of the major recommendations of the Moynihan Commission and includes a consideration of how some of these recommendations could be incorporated into the design of Australian access schemes or imported into the jurisprudence and day to day administration of FoI. A summary from the Commission's report, of the major reviews of US secrecy, has been included at the end of this article.

Background

The Moynihan Commission was established by the US Congress in 1995 to consider ways of reducing government secrecy in general whilst improving the protection of information essential to national security. The Commission concluded that:

The challenge of reducing secrecy overall and protecting secrets more effectively has increased since that time with the broadening reach of national security concerns. Even as the Freedom of Information Act (FOIA) has created a means for the public to obtain government information, consistent with security requirements, the reach of government secrecy has expanded in line with broadened conceptions of what must be protected in the name of national security. Moreover, although the current executive order on classification places a greater burden on those who seek to classify information, existing incentives still tend to promote secrecy over openness.

The result today is a system which neither protects nor releases national security information particularly well. Substantial concerns exist with respect to both the ability of the classification system to protect secrets effectively and the adequacy of the procedures in place to make information available to those outside the Government. In part, this is because the protection of government secrets and the reduction of government secrecy too often have been viewed as competing objectives, instead of being seen as able to reinforce one another when practised effectively. [p.1]

Establishment of a classification and declassification system (p.14)

The Commission recommended the enactment of a statute establishing the principles on which classification and declassification programs could be based. The following framework for such a statute was suggested:

1. Information is classified only if there is a demonstrable need to protect the information in the interests of national security, with the goal of ensuring that classification is kept to an absolute minimum consistent with these interests.
2. Procedures and structure for the classification of information will be established, as well as resources allocated for declassification. Details of these programs should be made publicly available.
3. In establishing the standards and categories to apply in determining whether information should be or remain classified, such standards should include consideration of the benefit from public disclosure of the information, and should weight it against the need for initial or continued protection under the classification system. If there is significant doubt whether the information requires protection, it should not be classified.
4. Information shall remain classified for no longer than 10 years, unless the agency specifically recertifies that the particular information requires continued protection based on current risk assessments. All information shall be declassified after 30 years, unless it is shown that demonstrable harm to an individual or ongoing government activities will result from such release. Systematic declassification schedules should be established. Further, agencies should submit annual reports on their classification and declassification programs to Parliament.

In the USA it was also recommended by the Commission that there be established a National Declassification Centre to co-ordinate, implement and oversee the declassification policies and practices of the Federal Government. It is proposed that the Centre will report annually to the Congress and President on its activities and on the status of declassification practices by all Federal agencies that use, hold or create classified information.

The Australian implications

The idea of a classification and declassification process is appealing. If the objective of most parliaments, as set out in the second reading speeches and object clauses of Australian FoI legislation, is to make as much information available as possible, it seems sensible to make an initial determination when information is created, or acquired, as to its general status under FoI, i.e. will it be exempt or available.

It should be possible to require that at any one point the information holdings of an agency should not exceed a particular ratio of exempt to available information (for instance 5% exempt to 95% available or accessible on request). A rationing regime for exemptions would force agencies to make objective assessment of the need for classifying information as exempt well in advance of particular requests. If an agency wanted to cloak the operations of one of its areas in shrouds of secrecy it would have to then grant wider access to its other operations. If newer information was more sensitive, then an agency would need to reveal more detail of its historical transactions and deliberations.

At the moment agencies, at both State and federal levels, have the luxury of an unlimited supply of exemption cards to play. In addition there is no imperative or requirement for an agency to facilitate access to information. As John Ralston Saul argues access laws:

merely confirm the principle that everything is secret unless specifically decided otherwise. The citizen will know only what he specifically asks. Indeed, the right-to-know laws encourage increased retention of information. They drive experts to use greater cunning — to register their information in more disconnected ways, so that when it is fished out it will give away as little as possible of what else is in the water.¹

The FoI game is based on the premise that an agency can play its exemption card(s) in isolation from any wider considerations about its informational holdings. It is not surprising to find repeatedly at the lower levels of review poor statements of reasons (reflecting the often last minute selection of exemptions to block a request), constant substitution of exemptions (like the interchange bench for a football game), or last minute concession of access to the determined applicant at the door of the tribunal like a folding hand in bluff poker.

A rationing regime that forces agencies to plan their classification regimes carefully and imposes an opportunity cost on claiming exemptions under FoI would change the dynamics of the access game slightly in favour of the applicant.

'Life cycle' classification system for secrets (p.20)

The Commission suggests that in enhancing the understanding of classification and declassification decisions, the concept of a life cycle for secrets should be adopted. The Commission states:

All information, classified and unclassified alike, has a life span in which decisions must be made with respect to its creation, management and use. But the management of classified material should also involve the important consideration of whether information should be classified at all, and if so, for how long. Some information needs to be kept secret for a day; some for a year; some for a generation or more.

The Commission suggests that this 'life cycle risk assessment' of classified information should encompass an analysis at each stage of the information's 'life' of:

1. whether the information requires protection (given the risks, threats, and vulnerabilities to it) and if so, how much and for how long;
2. the public's right to know about the functioning of government and whether this outweighs the need for protection in a given instance;
3. the cost of protecting or declassifying the information.

The Commission notes that this approach recognises that consideration of these criteria may lead to different results at different stages of the life cycle. For example, the public benefit in knowing the information initially may be outweighed by the need for its protection, but later may carry greater relative weight and may require its release.

The Australian implications

The concept of 'life cycle risk assessment' would add an exciting dynamic to FoI proceedings. Currently some Australian jurisdictions in a relatively ad hoc manner incorporate this type of risk assessment into public interest tests. It would add a greater degree of accountability to the process if agencies had to specifically pinpoint for any exempt information its 'life cycle risk assessment'.

The rest of this article summarises the other major recommendations of the Commission's report.

Improving the initial classification system (p.37)

The Commission to ensure that classification is used more efficiently, recommended improving the initial classification of information by requiring classifying officials to weigh the costs and benefits of secrecy and to consider additional factors in the decision to make or keep something secret. The Commission recognised that the initial decision to classify information is not to be taken lightly:

The initial decision to classify is critical: it is the most important part of the life cycle of secrets, and the place where the entire regulatory process begins. The decision should be made sparingly, and then vigorously enforced.

Such additional factors to be considered during the classification decision include:

- actual intention and ability of an adversary to inflict damage (threat);
- ability to defend assets in the event of an attack (vulnerability);
- probability of loss given threat and vulnerability (risk);
- resources required to avoid or minimise risk (cost);
- interest of adversaries in obtaining this information (value of information);
- expected benefit of the information being publicly available (public release).

The Commission provides the example that in considering these factors an official could conclude that while information may fall within one of the specified categories eligible for classification and might cause damage to national security if it were to be released, the actual threat to that information or likelihood of compromise may be so low or non-existent that classification is not necessary. Further, it suggests that the costs of protecting a particular piece of information may be so high that they outweigh the possible advantages to be gained from its protection.

The Commission suggested that the issue for classifiers is not just to see if particular information can potentially fit within a category of material that is eligible for protection, but to analyse in the first instance whether information requires the protection afforded by the classification system.

Accountability for classifiers (p.34)

The Commission recommended that agencies take several steps to enhance the proficiency of classifiers and improve their accountability by requiring additional information on the rationale for classification, by improving classification guidance, and by strengthening training and evaluation programs.

Elements of this approach include:

- original classifiers should provide a detailed justification for each original classification decision;
- derivative classifiers should be required to identify themselves on the documents they classify;
- classification guides should be better developed, more definitive, and updated regularly and industry should participate in the preparation of guides affecting industrial programs;
- training should conform to minimum Executive branch standards;