

Freedom of Information

Review

ISSN 0817 3532

ISSUE No. 105

Contents

Articles

25 years of evolving information privacy law: where have we come from and where are we going?
by Michael Kirby 34

FoI as a United States' foreign policy tool: a carrot and stick approach
by Stephen Lambie 38

The Freedom of Information Act 2000 and whistleblowers in the UK: some reflections
by Stephen Homewood 43

◆ ◆ ◆

*Articles in the *FoI Review* that are refereed are marked by an asterisk.

Credits

The *Freedom of Information Review* is published six times a year by the Legal Service Bulletin Co-operative Ltd.

International Editorial Board

Thomas B. Riley
Harry Hammitt
Maevie McDonagh
Ulf Öberg
Melissa Poole
Alasdair Roberts

Australian Editorial Board

Jason Pizer
Anne Cossins
Kim Rubenstein
Bill Lane
Peter Wilmshurst
Helen Townley
Chris Finn

Editor: Rick Snell
tel 03 62 26 2062 fax 03 62 26 7623
email: R.Snell@utas.edu.au
Website:
<http://www.foi.law.utas.edu.au/>

Reporters

Peter Wilmshurst (NSW), Dannielle Evans (Vic.), Emma Sundborn (Cth)

Print Post approved PP:338685/00011

This issue may be cited as
(2003) 105 *FoI Review*

© LSB Co-operative Ltd 2003

Comment

This issue features three articles that look at information issues in different ways. The first, by Justice Kirby, looks at developments in privacy law over the past 25 years. His analysis of an international approach to privacy highlights the relative paucity of similar international and regional efforts on access to government or official information. Justice Kirby notes the importance which co-operation between lawyers, judges, experts, NGOs and other institutions played in the development of information privacy law over that period. Yet his concentration on information privacy draws attention to the necessity to contemplate these issues not only from a *privacy* perspective but from an *informational* perspective. This wider informational perspective allows citizens to make informed decisions and be better informed about the fundamental choices they and governments are going to make in areas from public safety, national security, data mining and mining to the challenges, threats and opportunities presented by convergence in media, technology and data management.

In the second article, Stephen Lambie demonstrates the insights to be gained from combining good journalism skills, a fresh look at historical trends and a comparative approach. The author examines one of the central issues of FoI development, namely whether jurisdictions should (or are under pressure to) adopt a variant of the US model or whether they should attempt to mould their FoI legislation 'to fit their own peculiar political inheritances and public service structures and cultures'. Lambie also notes the increasing contradiction between a US foreign policy that promotes 'its model as a global template for FOI' while adopting greater levels of secrecy within its own borders.

The third article is by Stephen Homewood and looks at the FoI/whistleblower nexus (looked at from a US context by Robert Vaughn in (2002) 99 *FoI Review* 29) from a UK perspective. The policy choices being made in the home of Westminster in regard to open government and whistleblowing are a drama that is still unfolding. Homewood, like Vaughn, explores the interesting paradox that if FoI Acts were effective there would be little recourse needed to whistleblowing in the public sector. Yet a common theme emerging in countries like Australia, New Zealand and Canada is that mechanisms like whistleblowing legislation are needed to ensure the proper and effective administration of FoI Acts. Otherwise, especially in areas involving politically sensitive requests, there is a potential for information to be hidden, destroyed or withheld despite there being no legal justification to do so, or administrative practices (involving delay, excessive fee charges and content manipulation) will be undertaken to defeat or defer the request for information.

Recent news

Requests under the Irish Freedom of Information Act will cost 15 euros each from July 7. Finance Minister Charlie McCreevy also announced that appeals against FoI refusals would cost 75 euros on internal review and up to 150 euros for an external review. If experience in other jurisdictions is any guide then these fee changes in Ireland will produce a significant decrease in the number of applications and requests for review. The audacity of governments in their capacity to undermine FoI legislation never ceases to amaze me.

Rick Snell

25 years of evolving information privacy law

Where have we come from and where are we going?

In the beginning

A forum on privacy issues in March 2003 affords me an opportunity to reflect on 25 years of the *Guidelines on Privacy* of the Organisation for Economic Cooperation and Development (OECD). The work of the Expert Group of the OECD that drafted the *Guidelines* began in Paris in 1978. At the first meeting I was elected to chair the Group. That event proved a pivotal point in my professional career. Not only did it involve me closely with a collection of brilliant antagonists in the development of the basic principles of information privacy that have since influenced the law in Australia,¹ New Zealand² and beyond, it also exposed me to a rude awakening to an aspect of law which, up to that time, had largely been neglected in my legal experience. At first hand, I saw the way in which international law and policy were made. True, the 'law' on this occasion was the 'soft law' of the OECD *Guidelines on Privacy Protection*.³ But the lesson was not lost on me. In a very short time, I discovered how:

- global technology was forcing the pace of international legal and policy developments;⁴
- such developments had very large economic, cultural, legal and safety implications;⁵
- despite the divergences caused by the causative factors, the necessity of finding common ground (or more accurately of avoiding radically different approaches to a common technology) provided a significant stimulus to the development of international norms; and
- the work of international bodies could actually be of practical help to domestic law-makers. Confronted by new, controversial, technological and potentially divisive problems, local rule-makers naturally looked to trusted international agencies and their expert bodies to give a lead that would provide a foundation for uniform, or at least compatible, national laws on topics of international concern.

An appreciation of the importance of globalisation and regionalisation for the law is a mind-opening idea. So far, it has proved elusive to most lawyers. Most are content to live in the calm backwaters of their own jurisdiction. Yet in the age of jumbo jets, of cyberspace, of the human genome, of space travel and global problems like AIDS and terrorism, municipal jurisdiction is increasingly coming under the challenge of global and regional developments. Amongst the emerging norms are the statements of universal fundamental human rights. Amongst the fundamental human rights is that established by Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), guaranteeing the right to privacy. Universal fundamental human rights contribute one of the most powerful ideas at work in the law today. The idea is not yet dominant, but the dangers of the alternatives will surely soon make it so.

Many lawyers, whose minds are still locked in the pages of their law school notes, written down before 1978 when the OECD Group on Privacy first gathered, may be

sceptical about these propositions. But, having seen the way international law is changing and impacting upon domestic jurisdiction, I am an evangelist for the truth. It beckons us to a new and different legal era, suitable to a new millennium in which lawyers and other specialists must find common ground and shared principles with colleagues in other countries. Privacy protection is one such topic.

The Privacy Commissioners of Australia, New Zealand and the region know this to be true. Indeed, the Privacy Commissioners of the world meet regularly to track the developments of technology, law, business and practice and to share experience and ideas. It is good that they do so. Nowadays, truly, privacy and data security are global topics. The technology laughs at paltry efforts to make them amendable to purely local laws.

Privacy in the courts

After I rejoined the mainstream of the practice of law in appellate courts in Australia, following my decade in the Australian Law Reform Commission, I was struck by the utility of the OECD *Guidelines* when issues of general principle concerning the flow of information came up for consideration. But I have also been struck by the fact (noted in the Australian Law Reform Commission report on *Privacy*)⁶ that the common law sometimes has difficulty in formulating general principles or effective remedies for privacy protection. This was especially surprising given the importance that the English, from whom the common law derived, normally attached to individual privacy as a value to be respected in society.

In 2001 a case came before the High Court of Australia in which submissions were made to the Court asking it to repair the omissions of the law and to invent a common law right to privacy to be upheld in Australia.⁷ It arose in a case that involved a claim to protect a corporation that asserted that, unless restrained, its privacy had been invaded, and would continue to be, by a media organisation. The case involved many interesting legal questions. It grew out of the action of an unidentified party planting a hidden camera in private premises belonging to the corporation from which was procured film, later partly telecast, showing the circumstances in which native animals were slaughtered for export as food.

I will not detail all of the legal complications that arose in the case. Some of them concerned the Australian Constitution and the 'right' to free expression in Australia that has been discovered as an implication from the system of representative democracy established by the constitutional text. Interestingly enough, the latest word on that implication was written in a case brought to the High Court by the Rt Hon David Lange, one-time Prime Minister of New Zealand.⁸ His affection for Australia was so strong that he was determined to leave a lasting mark on Australia's constitutional law; and he did.

For present purposes, the interest of the *Lenah Game Meats* case is two-fold. First, it signalled a growing interest on the part of some of the High Court judges (including myself) to reopen consideration of the general development of civil remedies for privacy invasion that, in Australia, was largely stillborn after a (possibly erroneous) misreading of the decision of the earlier High Court in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*,⁹ decided in 1937.

Yet the *Game Meats* case was not a particularly good vehicle to encourage a definitive re-exploration of the general idea of privacy protection. In so far as this would, in turn, be stimulated by the provisions of Art 17 of the ICCPR, that provision appears to relate only to privacy of the human individual. It does not seem apt to apply to a corporation or agency of government. Nevertheless, noticing a number of recent developments in United States law,¹⁰ where the Supreme Court has discerned a 'strong tide running in favour of the so-called right of privacy' and developments in New Zealand law,¹¹ Canadian law¹² and English law,¹³ it now seems possible that an Australian protection of privacy under the common law might be developed in a suitable case involving an established invasion of the privacy of a human being.

The second importance of the recent decision of the High Court of Australia, as noted by David Lindsay in an article that heroically attempted to analyse the various streams of opinion in that decision, was the disparity over fundamentals disclosed in the reasons of the several participating judges. Mr Lindsay remarked, somewhat sharply,¹⁴

Taking these considerations into account, it is suggested that the relatively ad hoc, somewhat chaotic reasoning of the High Court in the *Lenah* decision is an example of what can happen in a legal system that refuses to take individual rights seriously and that, as a result, has an inadequate legal framework for recognising and protecting individual rights. While judicial recognition of an Australian tort of privacy would improve the position of individuals under the general law, an adequate legal regime must await the extra-judicial development of a Bill of Rights. As this seems unlikely, it would seem that protection of rights and freedoms under Australian law is destined to be influenced indirectly by developments elsewhere. By this, I am referring mainly to European human rights jurisprudence, via its effect on substantive principles of English law, including confidentiality law. In this sense, the relatively unsatisfactory reasoning evident in the judgments in *Lenah* is symptomatic of fundamental weaknesses in the structure of Australian law, just as much as it is a reflection of fundamental differences of opinion among the members of the current High Court.

The United Kingdom courts, which in the past have been such an important source of the common law for courts in Australia, New Zealand, Hong Kong and elsewhere in the region, are now (as Mr Lindsay's comment notes) directly under the influence of the *European Convention on Human Rights*. This is now the case, directly, because of the *Human Rights Act 1998* (UK). That is why, in several recent discussions,¹⁵ the English courts have proved much more receptive to arguments about judicial protection for the privacy of individuals than was formerly the case.¹⁶

Those who look to the courts as a new and revived source of privacy law in common law countries, after a long sleep lasting most of the last century, can therefore probably take heart from the recent trend of judicial

authority. It would not be the first time that the courts have developed the common law in a kind of symbiosis with developments of statute law.¹⁷ In my view, a similar process has occurred in respect of the common law principle governing the right to reasons for administrative decisions at a time when so many statutes have been enacted, by legislatures in many countries, to spell out that right in recognition of contemporary social values that demand its fulfillment.¹⁸ So the only advice that I can offer on this interesting development on privacy protection in the courts is: watch this space.

Institutional developments

In the 25 years since the OECD Expert Group on Privacy met under the chandeliers of the Château de la Muette in Paris, there have been enormous changes in the world, and in the technology of information distribution and processing. So great have been these changes that, in May 1999, *The Economist*¹⁹ proclaimed on its cover: 'The End of Privacy'. It described, in vivid detail, the features of 'the surveillance society' that had led it to this gloomy diagnosis.

Nothing that has happened in the four years since that declaration has reduced the problem which that distinguished newspaper called to notice. On the contrary, the Internet has continued to expand rapidly, the use of the World Wide Web more than doubling every 12 months.²⁰ William Gibson's vision of cyberspace comes ever closer.²¹

The particular difficulties of reconciling this new zone of human knowledge and activity were well illustrated by yet another recent decision of the High Court of Australia involving a defamation claim brought in Victoria for a news story uploaded on the Web in New York or New Jersey in the United States of America.²² The case vividly illustrates, once again, the difficulty, glimpsed as through a glass darkly by the OECD Group 25 years ago, of stamping national legal regimes upon transborder flows of data.

Three and a half years ago, at the 21st international conference on privacy and personal data protection in Hong Kong, I examined the extent to which the 1980 OECD *Guidelines* remained relevant and useful in these new technological circumstances and the extent to which they were showing signs of their age.²³

One of the greatest challenges to the effectiveness of the *Guidelines* has been the provision of extensive indexes on Internet sites such as *Yahoo!* and the *Altavista* search engine. The *Guidelines* of 1980 were prepared on the environment of the technology then known. That was before webcrawlers, spiders, robots and trawlers were invented that, in the context of the Internet, could subject personal data to fresh surveillance against criteria different from those for which the data had originally been collected and possibly unknown or even non-existent at the time of such collection.

It was these changes that led me to a number of suggestions for new privacy principles relevant to contemporary technology. I listed them in late 1999. All of them remain relevant today.²⁴

- a right in some circumstances not to be indexed;
- a right in some cases to encrypt personal information effectively;²⁵
- a right to fair treatment in key public infrastructures so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy;
- a right, where claimed, to human checking of adverse automated decisions and a right to understand such decisions affecting oneself;²⁶ and
- a right, going beyond the aspirational language of the 'openness principle' in the OECD *Guidelines*, of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned.²⁷

The growth of e-commerce has led to concern amongst computer and Internet users both about privacy and security of personal data, a point noted by Stephen Lau, former Privacy Commissioner of Hong Kong.²⁸ The right of users to be informed in advance of the provider's policy on data privacy and to have a choice of anonymity for browsing and transacting business, encryption and collection and use of sensitive data is also a subject of expressed concern. The provider may have current strategies and policies that are indeed communicated to the user. Yet these are always subject to supervening obligations imposed on the provider by law for the purpose of enforcement of new criminal offences (eg access to prohibited pornographic Websites, intellectual property protection and revenue gathering).

In addition to these considerations, the advance of the Human Genome Project to its effective completion, ahead of schedule, in 2003 coincides with yet another important contemporary anniversary — the 50th commemoration of the first description by Watson and Crick on 28 February 1953 of the elements of DNA.

The potential use of DNA and modern systems of genetic data to provide a vast range of sensitive health data about the individual, as well as a secure and virtually unique means of identifying the individual, presents large and puzzling questions for privacy protection in the future. Such questions will occupy privacy commissioners, law reform agencies, policy makers and legislators in the years ahead.

Amongst the questions that are raised by the use of DNA in this connection are those concerning:

- non-consensual DNA testing;
- consensual DNA testing solely for research;
- use of discarded or other DNA for purposes of health, employment, insurance and criminal record checks;
- collection of data based on DNA material that profoundly affects the life choices of the individual concerned; and
- invasion of genetic data banks and unauthorised dissemination of genetic data about the individual.²⁹

Little wonder that actual and potential misuse of genetic information has already occurred. The Australian Law Reform Commission has signalled its continuing involvement at the cutting edge of these issues. In August 2002 it published a Discussion Paper of nearly a thousand pages dealing with a vast range of questions concerned with access to genetic testing; the use of information and

health data; the need for anti-discrimination law; the requirement for enforcing the *Australian National Statement on Ethical Conduct in Research Involving Humans*; the encouragement of best practice in human genetic research; special rules for human tissue collection, the ownership of human genetic samples, the establishment of genetic registers; the provision of genetic counselling and medical education; the conduct of genetic screening; the use of genetic data for discrimination in insurance and employment; the availability of DNA parentage testing; the use of DNA in immigration decisions, forensic procedures, criminal investigation, post-conviction activity and civil proceedings.

The foregoing list provides an indication of the enormous variety of questions that will need to be tackled.³⁰ The final ALRC report on these topics was provided to the Federal Attorney-General in April 2003. It was released in late May 2003 following its tabling in Federal Parliament.³¹ It follows the lines foreshadowed in the Discussion Paper.

Terrorism and privacy

During 2003 it has also been impossible to ignore the implications for the protection of privacy and other civil liberties of the global response to acts of terrorism and the dangers of the misuse of weapons of mass destruction. Early in the year the world watched with concern and mixed feelings the conflict and post-war settlement in Iraq. The conflict was a direct result of the extraordinary events in the United States of 11 September 2001 when many accepted features of the world changed.³²

In consequence of such changes, laws have been enacted or proposed in many countries, including Australia. Such laws and the practices that have gathered around them, have been designed to enhance the capacity of societies to respond to the perceived dangers of terrorism and breaches of national security and of the criminal law. Enhancement of the power of police and of national security agencies has obvious implications for the legal protection of individual privacy. In a time of war or of terrorism, there is a tendency, if not for the law to fall silent, at least for its defence of basic civic freedoms to become somewhat confined.

From the point of view of privacy regulators, the issues arising from such anti-terrorism laws are highly relevant to the purposes for which they have been established. However, they tend to remain on the fringes of the jurisdiction of privacy agencies, given the wide exemptions typically found in their legislative powers so far as they concern national security and intelligence activities. Such exemptions have not, however, prevented some privacy guardians from raising their concerns about the over-reach of proposed security laws.

Some have done so in private, knowing that, in the current sensitive climate, their views on such subjects, if expressed in public, are likely to be marginalised or ignored. On the other hand, some Privacy Commissioners (whom Lord Denning would doubtless have described as 'bold spirits') have felt entitled, or even obliged, to make public comment on this topic. Thus the Canadian Privacy Commissioner, Mr George Radwanski, has challenged

the Canadian Government on several issues arising out of this concern. By doing so, he has raised the profile of the debate in Canada on the inter-relationship of privacy protection and security protection.

In the Commissioner's overview published with the Privacy Commissioner of Canada's *Annual Report* to Parliament, released in January 2003, Mr Radwanski remarked.³³

It is my duty ... to report a solemn and urgent warning to every Member of Parliament and Senator and indeed to every Canadian. The fundamental human right to privacy in Canada is under assault as never before. Unless the Government of Canada is quickly persuaded from its present course of parliamentary action and public insistence, we are on a path that may well lead to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it. We face this risk because of the implications, both individual and cumulative, of a series of initiatives that the Government has mounted or is effectively moving forward. These initiatives are set against the backdrop of September 11, and anti-terrorism is their purported rationale.

Specifically, the Canadian Commissioner questioned the creation of new 'Big Brother' passenger data bases for international transport movements; the dramatic enhancement of official powers to monitor individuals' communications; a suggested introduction of a national ID card containing biometric identifiers; and support for video-surveillance of public streets by the Royal Canadian Mounted Police.³⁴

The Commissioner's report includes blunt speaking, critical of proposed Canadian legislation for a *Public Safety Act* of changes to the *Criminal Code* and of the introduction of practices to increase the surveillance of persons in and out of Canada. He acknowledges fully the dangers that terrorists present to freedom and civic values, including privacy. But he urges that Canadian society must remain faithful to the tolerant values that terrorism seeks to attack. Otherwise, he points out, the terrorists will have succeeded in their basic challenge to our freedoms.

These remarks are clearly deserving of close attention.³⁵ In most countries, including Australia, legislation is under active consideration to enhance official powers having unmistakable implications for individual human privacy.

In the same spirit as the Canadian Commissioner, the American Civil Liberties Union (ACLU), in January 2003, issued a report warning of the growth of the surveillance society in the United States. That report *Bigger Monster, Weaker Chains*³⁶ is relatively brief. It provides a useful synthesis of developments in video surveillance, data surveillance, genetic privacy, biometrics, communications technology, government data bases and the extension of the power of government agencies. The thesis of the ACLU report is that 'we are being confronted with fundamental choices about the sort of society we want to live in'.³⁷

The ACLU report draws to notice a recent decision of the Supreme Court of the United States in *Kyllo v The United States*,³⁸ decided after 11 September 2001. There the Court held that a reasonable expectation of privacy could not be determined by the power of new technologies. In a decision written by Justice Antonin Scalia, the Supreme Court held that, without a warrant, the police

could not use a new thermal imaging device that searches for heat sources to conduct what was the functional equivalent of a warrantless search for marijuana cultivation in Mr Kyllo's home. Specifically, the Court declined to leave the privacy of that home 'at the mercy of advances in technology'.³⁹ There will be more such cases of this kind before the courts. In many countries, such as Australia and New Zealand, there are no constitutional protections equivalent to those successfully invoked in the United States.

Getting the balance

Obviously, getting the balance between the protection of the claims and interests of society and the protection of individual privacy has never been easy. In an age of civic danger and terrorism, keeping cool heads and preserving the proper equilibrium will surely be one of the great challenges for privacy agencies in the years before us. So much seems to conspire against the defence of individual privacy. But this fact merely makes it all the more important that we defend and uphold this cherished human right and precious feature that belongs to every individual in accordance with international human rights law.

THE HON JUSTICE MICHAEL KIRBY AC CMG

The Hon Justice Michael Kirby AC CMG is Justice of the High Court of Australia; one-time Chairman of the Australian Law Reform Commission; Chairman of the OECD Expert Group on Transborder Data Flows and the Protection of Privacy and of the OECD Expert Group on Data Security.

This article was adapted from an address to the Privacy Issues Forum, Parliament House, Wellington, New Zealand, 28 March 2003.

References

1. *Privacy Act 1988* (Cth).
2. *Privacy Act 1993* (NZ). The Act became fully operational in July 1996.
3. OECD, *Guidelines on the Protection of Privacy and Transborder Data Flows* (Paris, 1981).
4. Kirby, M.D., 'Access to Information and Privacy: The Ten Information Commandments' (1987) 55 *Cincinnati Law Review* 745 at 750-51
5. Rees, M., 'The Final Countdown', *New Scientist*, 3 May 2003, p.33.
6. Australian Law Reform Commission, *Privacy*, ALRC 22, 1983.
7. *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
8. *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
9. (1937) 58 CLR 479.
10. *eg Cox Broadcasting Corporation v Cohn* 420 US 469 at 488-489 (1975).
11. *eg P v D* [2000] 2 NZLR 590 at 599-601; Tobin, R., 'Invasion of Privacy' [2000] NZLJ 216. See also *Lenah Game Meats* (2001) 208 CLR 199 [325] and New Zealand Law Commission, *Protecting Personal Information from Disclosure*, Preliminary Paper 49, 2002.
12. Linden, A., *Canadian Torts Law*, 6th edn, 1997, p.56; *Aubry v Duclou* (1996) 141 DLR (4th) 683.
13. *R v Broadcasting Standards Commission; Ex parte BBC* [2001] 3 WLR 1327; cf *Lenah Game Meats* (2001) 208 CLR 199 [326].
14. Lindsay, D., 'Protection of Privacy Under the General Law Following *ABC v Lenah Game Meats Pty Ltd*: Where to Now?' (2002) 9 *Privacy Law and Policy Reporter* 102 at 107.
15. *eg Douglas v Hello! Ltd* [2001] 2 WLR 992.
16. A point noted by Gummow and Hayne JJ in *Lenah Game Meats* (2001) 208 CLR 199 [112]-[116].
17. *Cotogno v Lamb [No 3]* (1986) 5 NSWLR 559 at 570-572; but see *Lamb v Cotogno* (1987) 164 CLR 1 at 11.
18. cf *Osmond v Public Service Board* [1984] 3 NSWLR 447 at 465. But see *Public Service Board (NSW) v Osmond* (1985) 159 CLR 656 at 669-670 and see now *Baker v Minister of Citizenship and*

- Immigration* [1999] 2 SCR 815; *Mukherjee v Union of India* [1990] Supp 1 SCR 94.
19. 1 May 1999, 11, pp.17-19. See also Varney, C., 'The Death of Privacy?', *Newsweek Special Edition*, Dec 2000-Feb 2001, pp.78-79.
 20. Miller, R., 'The Internet in Twenty Years: Cyberspace the New Frontier,' OECD, Paris, 1997; cf Kirby, M.D., 'Privacy in Cyberspace' (1998) 21 *UNSW Law Journal* 323; Bygrave, L.A. *Data Protection Law*, Kluwer, 2002, p.29; Longworth, E., 'The Possibilities for a Legal Framework for Cyberspace — Including a New Zealand Perspective' in UNESCO, *The International Dimensions of Cyberspace Law*, Vol 1, Ashgate, 2000, p.9.
 21. Gibson, W., *Neuromancer* cited in Frank, E., 'Can Data Protection Survive in Cyberspace?' (1997) 8(2) *Computers and Law* 20.
 22. *Dow Jones and Co Inc v Gutnick* (2002) 77 ALJR 255.
 23. Kirby, M.D., 'Privacy Protection — A new Beginning' (2000) 18 *Prometheus* 125 and in papers of Hong Kong, Office of the Privacy Commissioner for Personal Data, *Privacy and Personal Data, Information Technology and Global Business in the Next Millennium*, 1999, p.2.
 24. cf Victorian Law Reform Commission, *Defining Privacy*, 2002.
 25. OECD, *Guidelines for Cryptography Policy*, Paris, 1997, 27 OECD Doc C, 1997, 62/Final. cf Adams, J., 'Encryption: The Next Best Thing?' (1998) 2 *Computers and Law* 39 at 40.
 26. Greenleaf, G., 'Privacy Principles — Irrelevant to Cyberspace?' (1996) 3 *Privacy Law and Policy Reporter* 6 at 114, 118.
 27. Clarke, R., 'Profiling and Its Privacy Implications' (1994) 1 *Privacy Law and Policy Reporter* 7 at 128-9; Wacks, R., 'Privacy in Cyberspace: Personal Information, Free Speech and the Internet', in P Birks (ed) *Privacy and Loyalty*, Oxford, 1997, p.93.
 28. Lau, S., 'E-Commerce, Consumer Rights and Data Privacy, 3rd Quarter, 1998 *I-Ways*, 37 at 38; cf Gamertsfelder, L. & Ors, *E-Security*, Lawbook Co, 2002.
 29. Curley R., and Caperna, L., 'The Brave New World is Here — Privacy Issues and the Human Genome Project', (2003) 70 *Defense Counsel Journal* 22-35.
 30. Australian Law Reform Commission, *Protection of Human Genetic Information* (2002) (DP 66). The International Bioethics Committee of UNESCO is preparing an *International Declaration on Human Genetic Data* which is expected to be placed before the General Conference of UNESCO in October 2003. This elaborates the UNESCO *Universal Declaration on the Human Genome and Human Rights*, 1997.
 31. Australian Law Reform Commission, *Essentially Yours — The Protection of Human Genetic Information in Australia*, ALRC 96, 2003.
 32. Williams, G., 'One Year On — Australia's Legal Response to September 11' (2002) 27 *Alternative Law Journal* 212 referring to Security Legislation Amendment (Terrorism) Bill 2002 (Cth).
 33. Canada, Privacy Commissioner, *Annual Report to Parliament 2001-2002*, Commissioner's Overview.
 34. *Ibid*, 2.
 35. Kirby, M.D., 'Australian Law — After 11 September 2001' (2001) 21 *Australian Bar Review* 253, contrasting the decisions of the High Court of Australia in *Australian Communist Party v The Commonwealth* (1951) 83 CLR 1 and the Supreme Court of the United States in *Korematsu v United States* 323 US 214 (1944) and *Dennis v United States* 341 US 494 (1950).
 36. American Civil Liberties Union, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*.
 37. *Ibid*, 15.
 38. 533 US 27 (2001).
 39. *Kyllo v United States* 533 US 27 (2001).

FoI as a United States' foreign policy tool: a carrot and stick approach

The response of the United States' Federal Administration to the terror attacks of September 11, 2001 has seen history repeat itself through the revival of a deeply-rooted double standard in relation to freedom of information. On one hand United States' state and federal governments have responded to the attacks by restricting access to a huge range of government-held information on the grounds that it might assist terrorists. On the other, the United States' Federal Administration has reinvigorated and old policy of heavily promoting its, often inappropriate, model of FoI around the world.

An insight into the contradiction becomes evident if one delves beneath the surface of United States' foreign policies. As a starting point, it is instructive to compare a directive issued by Bush Administration Attorney General John Ashcroft in October 2001 with a memorandum by Clinton Administration Attorney General Janet Reno in 1999. In her statement Reno had called for 'maximum responsible disclosure of government information'. Further, she urged public servants to 'consider whether they can make a discretionary disclosure of a requested record or portion of a record even though it falls within one of the [FoI] Act's exemptions'.¹ Ashcroft's directive superseded Reno's. Posted on the Department of Justice's Office of Information and Privacy (OIP) Web site, it took an opposite stance and said, in part:

Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.

And:

When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.²

The federal policy backflip has also impacted on attitudes to FoI in many states. The flow-on effect was well summarised by United States' Pew Centre journalist Kathleen Murphy who wrote:

Many state officials have followed Ashcroft's lead, arguing that restricting public access to many kinds of information will help prevent future attacks by hampering terrorists' activities. But civil rights groups and journalists counter that many of the restrictions have little to do with preventing terrorism.

A dozen states — Alaska, Connecticut, Florida, Idaho, Louisiana, Maine, Michigan, New Hampshire, Ohio, South Carolina, Utah, and Virginia — have adopted new rules to limit access to public records in the name of national security this year [2002].³

Yet while United States' authorities were attempting to limit the availability of information at home — and particularly information which could be freely accessed via the Internet — they were urging the administrators of other nations to be much more open. That paradox comes sharply into focus when Ashcroft's policy reversal is viewed in terms of another posting on the Department of Justice's OIP Web site in late 2002. Headed 'OIP Gives FOIA Implementation Advice to Other Nations,' the notice boasts, in part:

As it is United States government policy to encourage the adoption and successful implementation of openness-in-

government (or 'transparency in government,' as it often is referred to overseas) throughout the world. OIP has provided background briefings and advice to increasing numbers of foreign visitors over the years. To date, more than 45 other nations have enacted their own Freedom of Information Act counterparts, with many more considering such legislation, and OIP has met with representatives of more than six dozen nations.

Most recently, the nations of Japan, Mexico, and the United Kingdom have enacted major freedom of information legislation, the implementation of which is of great concern to those countries, and OIP has been actively supportive of those efforts. Japan's 'transparency' law took effect on April 1, 2000, Mexico's takes effect on June 10, 2003, and the UK's is now scheduled to take effect on January 1, 2005.⁴

An old policy revived

It is generally acknowledged that United States' freedom of information legislation has been adopted to varying degrees as a blueprint by many other nations which have introduced Fol statutes since 1966. However, it is much less well known outside United States' government circles that since World War I and particularly after World War II, Fol has been regarded by successive United States' administrations as a key foreign policy tool. Neither is it generally known that the latter agenda led the United States Department of State to attempt to impose Fol on other nations in an obsessively ethnocentric, if arguably altruistic, carrot-and-stick style campaign in which governments — including some Westminster-style governments — were offered incentives and/or threatened with sanctions in a bid to encourage compliance.

Details of how that campaign originated were documented in an obscure but still highly relevant 1948 Department of State publication, *Freedom of Information in American Policy and Practice*.⁵ A fascinating 65-page 'pamphlet' compiled by two members of the Foreign Policy Studies Branch of the Department of State's Division of Historical Policy Research, the document was prepared less than three years after the world had emerged from the horror of World War II. The impact of war on personal and press freedoms and the broad thrust of United States' policy relating to Fol were explained in the foreword to the report, which says:

Although the proper limit of freedom is a matter on which opinions differ, wide recognition is given in principle to the responsibilities of society, and of government in particular, for the maximisation of four fundamental liberties made famous as a group by Franklin D Roosevelt. The first, freedom of expression, enjoys the theoretical adherence of all governments, but practice lags behind theory in respect to this principle as in the case of many other broad tenets of human justice.

The policies of our government affecting freedom of information have a long and creditable history. With occasional aberrations, domestic freedom of information has generally prevailed over opposing tendencies. In the international domain, the United States has conducted negotiations both bilaterally and multilaterally in the effort to ensure the unhampered communication of knowledge.

It is hoped that this pamphlet, reviewing the history of American policy and practice as regards freedom of information, will stimulate constructive thought on the problem of making free expression a reality throughout the world, for now more than ever success in advancing the solution of mankind's problems depends upon the spread of knowledge and understanding throughout the world.⁶

Ironically, however, at the time the document was written the United States did not have a functioning Fol system of its own. Congress had enacted precursor legislation in the form of its *Administrative Procedure Act* of 1946 which made it compulsory for all federal agencies 'to keep and maintain records which were to be open to inspection by the public'.⁷ But it would be nearly 20 years before the initial 1946 law was complemented with a workable Fol statute, which was not implemented until mid-1967.

Treaties and sanctions

Despite the apparent hypocrisy of the United States in trying to foist Fol on the world many years before it was to enact a properly functioning model of its own, there can be no doubt about the Department of State's enthusiasm for the cause. In its 1948 report the department explained its reasoning in the following terms:

In recent years ... the problem of international freedom of information has increasingly taken the stage.

The international aspects of the problem have loomed large in the minds of Americans because of the evident relation (sic) of world-wide press freedom to the promotion of understanding between peoples and to the maintenance of universal peace. If war is to be avoided and if international co-operation is to be a living reality, world opinion must play its proper role as arbiter in the peaceful settlement of the international differences which will naturally arise. World opinion, however, can exercise its influence towards peace and cooperation only in so far as the peoples of the world are able to receive uncensored news and to express their thoughts and feelings without fear.⁸

It is therefore significant that the approach to Fol in the United States was initially seen in other nations as being more correlated with an ethnocentric United States' perception of media freedom than with the promulgation of individual rights. Further, Fol developed in the United States in a spasmodic, sometimes tortuous, cycle in which rights were suppressed in times of conflict followed by advances in times of peace. In fact, in a frank admission, the Department of State report acknowledged that there had been a draconian over-reaction in the United States in the extent to which free speech was stifled in the more than 30-year period from the start of World War I to the end of World War II. In a statement that could equally have been made in the wake of the Bush Administration's response to the September 11, 2001 terrorist attacks on New York and Washington, the report suggested:

War always involves restrictions on individual liberty of action, and one of the prices paid by the United States for its [from April 1917] participation in World War I was a marked decline in popular regard for freedom of speech and other civil liberties. Both federal and state laws in this field are regarded as having gone beyond military necessity and the demands of national safety.⁹

The report then boasted that:

In the words of President Woodrow Wilson, the United States took part in World War I in the hope of making the world 'safe for democracy'. Convinced that among the causes of war were the secret negotiations and secret agreements between countries, President Wilson included one aspect of freedom of information in his fourteen-point program for a lasting peace, which he unfolded to Congress on January 8, 1918. ...

In the peace treaties themselves, certain clauses bore specifically on freedom of information.¹⁰

Similarly, peace treaties and conventions signed after the end of World War II by the governments of Japan, Germany, Italy, Rumania, Hungary and Finland all contained clauses inserted at the behest of the United States which promoted fundamental domestic freedoms including those of free speech, religious worship, assembly, expression and the press.¹¹ As if to reinforce the point, the 1948 Department of State report blatantly, even proudly, noted that:

Largely at the instance (sic) of the Congress of the United States, the threat of economic sanctions has been developed since 1945 as a weapon for promoting freedom of information.¹²

And:

The Department of State has determined to take advantage of all opportunities to promote freedom of information through bilateral channels by such means as treaties dealing exclusively with freedom of information and separate articles or clauses on this subject in treaties of commerce and navigation, trade agreements, and cultural agreements.¹³

The policy was extended after the United Nations was founded as a replacement for the League of Nations on 24 October 1945.¹⁴ As one of five permanent members of the Security Council, the United States ensured that Fol 'articles and clauses' were also included in post war international trusteeship agreements, with the Department of State boasting:

Eight suggested trusteeship agreements were referred to the United States [by the United Nations] in 1946 for comment. They covered the terms under which the Governments of Australia, Belgium, France, New Zealand, and the United Kingdom proposed to administer certain territories [such as Papua New Guinea] already held by those nations under League of Nations mandates. Among the important provisions suggested by the United States and incorporated in the agreements before they were finally approved is the clause in each agreement protecting 'freedom of speech, of the press, of assembly, and of petition'.¹⁵

Fol and the United Nations

The report also makes it clear that as a direct result of heavy United States' pressure, the promotion of Fol and press freedom had actually become fundamental founding platforms of the United Nations — something reflected in a speech by United States' Assistant Secretary of State Adolf Berle to the Foreign Press Association in New York in June 1944 during which Berle said:

... freedom of information is a major necessity if world organisation is to succeed. With freedom of information there is possibility of understanding between peoples. Without it the way is always open to build up misunderstandings, suspicion, fear, and finally, hatred. Often a knowledge of the facts ends the suspicion; a square look at the situation allays fear; and except in rare cases, few people hate where they are fully informed.¹⁶

The 1948 Department of State report leaves no doubt that the United States' Government and the American Society of Newspaper Editors went to extreme and obsessive lengths in promoting the cause of Fol in the United Nations. The document explains, for example, that even before the United Nations Commission on Human Rights had been established, the United States' Secretary of State sent a telegram to the American Society of Newspaper Editors giving an assurance:

... that as soon as the Commission on Human Rights was formed the United States Government would urge it to undertake a study of the means for promoting freedom of the press, freedom of communication, and a fuller flow of knowledge and information among all peoples.¹⁷

But the United States did not even wait that long. It began beating the drum as hard and loudly as it could after establishment of the forerunner to the Commission on Human Rights, the so-called 'nuclear Commission on Human Rights'. The latter body met for the first time in April 1946 with Mrs Eleanor Roosevelt, the widow of former President Franklin D Roosevelt,¹⁸ in the chair.¹⁹

Fears of cultural imperialism fuel a backlash

On 8 May 1946 the nuclear Commission on Human Rights resolved to recommend to the full commission, when it was established, that it should establish a sub commission on freedom of information and the press. The sub commission was established in 1946 but did not meet until May 1947. In the interim, however, the United States' Government through the Department of State had been quick to recognise that the formation of the United Nations Educational, Scientific and Cultural Organisation, UNESCO, in November 1946, provided another opportunity to push its Fol barrow even further as a foreign policy tool. In doing so it lobbied the inaugural UNESCO conference to advance three specific proposals. In summary they were: (1) That UNESCO should co-operate with the United Nations Commission on Human Rights in preparing a report on obstacles to the free flow of information and ideas around the globe, (2) That experts be appointed to 'comprehensively study the possibility of a world-wide radio network', and (3) That UNESCO try to find ways of improving, extending and cutting the cost of 'services to the press and radio by cable, wireless and mail'.²⁰ But the United States' delegation was about to receive a rude shock, the nature of which was forthrightly explained in the 1948 Department of State report as follows:

The first session of the general conference of UNESCO met at Paris from 19 November to 10 December 1946. Thirty governments, including the United States, were officially represented; and 18 additional governments sent observers. Eleven intergovernmental organisations sent observers also, as did 70 non-governmental international agencies. The United States delegation noted, in its report to the Secretary of State [after the event], that 'there was an initial and, to Americans, a rather surprising hostility to the use of mass media for international understanding'. Much of this hostility derived apparently from a fear that the free employment of facilities of this character would permit the nations most advanced in the technique — particularly the United States — to use the new means of communication for the purpose of 'cultural imperialism' which would form the cultures of the world in the image of Hollywood.²¹

Two years later, in 1948, with the United Nations and UNESCO having failed to act on a United States' offer to establish a world-wide radio network that would use the facilities of the Voice of America — which had been established in 1942 as 'a means of fighting the Cold War'²² — to broadcast 'educational, scientific and cultural programs', and with its push for Fol becoming hopelessly bogged-down within the United Nations' General Assembly, the Department of State was forced to admit it was facing the emergence of 'major problems' hindering 'efforts to promote freedom of information on a world-wide basis'.²³ Among those difficulties was the tricky question of:

How may we lessen the resistance against the American concept of freedom of information, such as the views of those who fear American 'cultural imperialism' (the hypothetical victory of American comic strips and of 'Hollywood' over the local cultural heritage) and the desire of various countries to protect their mass media industries against competition with the preponderant facilities of the United States?²⁴

The Department of State admitted it was facing other difficulties, too, such as how to 'best promote the entry of American periodicals, books, and films into foreign countries', how to 'obtain the privilege' of sending foreign correspondents abroad to places 'from which the American public wants more news', and 'how may we ensure the receipt in this country of unexpurgated reports from American correspondents abroad'.²⁵ Little wonder then, especially in the climate of an escalating cold war with the USSR, that United States' Fol initiatives were pushed to one side in the United Nations and finally sank in a sea of suspicion in the early 1950s.

State governments set the agenda for domestic Fol

But despite the setback in the United Nations and a less than enthusiastic reception from some public servants at home, pressure for domestic Fol laws was increasing within the United States. A Freedom of Information Centre was established at the University of Missouri in 1958. By 1960 about 30 states had passed 'open meeting laws' which decreed that meetings of government boards, commissions, and councils must be open to the public, with it reported that 'about half these laws also called for free access to records'.²⁶ Finally, the federal *Freedom of Information Act* was signed into law on July 4 (Independence Day) 1966 by President Lyndon Johnson. It became effective exactly one year later.²⁷ With the United States starting to practise what it had been preaching in relation to Fol, pressure then started to be exerted on governments around the world to allow their citizens similar rights. A little over a decade later Fol was openly back on the agenda in the United States as a foreign policy tool. In 1981 an article headed 'Information Policy Around the World' was published in the United States' Department of Justice publication *FOIA Update*. It boasted that:

After the *Freedom of Information Act* was adopted in the United States, five other nations established laws allowing public access to government records. Denmark and Norway enacted legislation in 1970; Austria, in 1974; Holland and France followed in 1978. ...

At least five nations are in various stages of pursuing freedom of information policy.²⁸

Remembering that the article was written in 1981 and that Australia, Canada and New Zealand all introduced Fol statutes into their parliaments in 1982, it is significant that the *FOIA Update* article then considered the Fol 'Situation in Canada', 'Action in Australia', 'The Japanese Experience', 'In Great Britain' and commented on the fact that there was an expectation Fol legislation would be introduced in New Zealand later that year. The author subsequently concluded:

Thus, there is a growing trend among parliamentary democracies around the world to establish a legal right of public access to government records. **The American Freedom of Information Act is an important model for these nations in their pursuit of such policy. Indeed, in developing and**

administering the FOIA, the United States enjoys a leadership role which may be apparent only outside of our own borders.²⁹ [emphasis added]

United States influence on Fol in Australia

Thus the collective memory and fears of 'cultural imperialism' having faded, many nations adopted modified versions of the United States' FOIA. How they were encouraged to adopt that model was typified in the Australian experience. Its federal statute had its genesis in an election campaign in 1972 when then leader of the Australian Labor Party opposition, Gough Whitlam, promised to enact Fol legislation 'along the lines of that operating in the United States' if his party won.³⁰ After subsequently being elected the Whitlam government started preparing what it said would be its Fol legislation. Then federal Attorney-General Senator Lionel Murphy put a submission to cabinet on Fol in January 1973. The submission advocated rejection of the Swedish model of Fol (which remains the most open and workable in the world) and endorsement of the United States' version.³¹ Murphy later announced that the government's Legislation Committee would report on 'any modifications to the United States' *Freedom of Information Act 1966* appropriate for legislation in Australia'.³² However, Snell reports that within 10 days of Murphy's announcement, the carriage of the cabinet's decision on Fol had mysteriously passed from the Legislation Committee to an inter-departmental committee composed of senior public servants.³³ Interestingly in the current context, that committee was advised for a short time in 1973 by then General Counsel for the United States' Civil Service Commission and former member of the United States' Department of Justice in charge of administering his nation's Fol Act (FOIA), Anthony Mondello. When the committee report was tabled in Federal Parliament in 1974, it suggested 'it would be necessary to modify the United States' legislation to take account of Australia's constitutional and administrative structure'.³⁴ In the end, however, the Whitlam Government lost office before it had even prepared draft Fol legislation.

Interestingly, the issue might have rested there if Whitlam's conservative successor Malcolm Fraser had not adopted Fol as Liberal Party policy. Marsh recounts that Fraser convened a 'further inter-departmental committee' — which just happened to have the same membership as the Whitlam-era committee — to 'consider the report of the previous committee' with particular regard to the 1974 amendments to the United States' *Freedom of Information Act*.³⁵ After years of discussion, arguments and reports a bill was finally drafted. It eventually became law on 1 December 1982.³⁶ But the legislation was seriously flawed. Its loose wording and its complex and vague exclusions and exemptions made a direct comparison with the United States' legislation it was based on impossible. In addition, the Australian law had to operate in a Westminster style system, a far cry in many ways from the United States' republican regime.

Threats of sanctions resurface

Systemic differences, however, do not seem to have damped the enthusiasm of those in the United States

Administration who revived the idea of FoI as a foreign policy tool. As recently as 2002 the threat of sanctions emerged again as a means of encouraging the global adoption of the United States model of FoI, even in nations with what amount to incongruously different systems of governance. For example, among the nations being pressured in recent times were signatories of the Inter-American Convention Against Corruption. The convention operates under the charter of the Washington-based Organisation of American States, which, in turn, is a regional agency of the United Nations.³⁷ In addition to the United States and Canada, its members include regimes as diverse as those in Colombia, Bolivia, Brazil, Nicaragua, Trinidad and Tobago, Venezuela, Peru, Uruguay, Mexico and Guyana. In some of those nations, for instance Colombia, pressure to introduce FoI has been specifically tied to United States foreign aid.³⁸ In July 2002 Privacy International reported that:

International bodies such as the Commonwealth, Council of Europe and the Organisation of American States have drafted guidelines or model legislation to promote freedom of information. The World Bank, the International Monetary Fund and other donors are also pressing countries to adopt access to information laws as part of an effort to increase government transparency and reduce corruption.³⁹

In that context, and looking back to the United States' push to have FoI adopted as a key platform in the foundation of the United Nations in the 1940s, it is of at least passing interest that the Organisation of American States operates under the umbrella of the UN. It is also of note that the World Bank was formed in 1947 to assist in post war reconstruction. It is based in Washington, its biggest shareholder is the United States, its president is a United States' citizen and it works closely with the United Nations.⁴⁰ The World Bank also has close ties with the International Monetary Fund, which is also based in Washington and is a 'specialised agency of the United Nations'.⁴¹

Little allowance for systemic differences

Finally, putting talk of sanctions aside but returning to the question of systemic differences, those in the United States and elsewhere who have pushed that nation's FOIA as a global model have overlooked the highly significant fact that the United States' FoI statutes evolved in a system with unique constitutional guarantees of personal and press freedoms, and in a system of governance and a political climate not found in other nations. In 1981 Canadian FoI advocate Donald Rowat specifically referred to plans by the federal governments of Canada and Australia to introduce FoI laws based on the United States' federal model. He predicted — correctly as it turned out — that each nation's laws would be 'weak'⁴² and said that the British political inheritance of each meant that:

It is significant that all of the governments in parliamentary systems that have sponsored or drafted an access law have produced weaker versions than the laws of Sweden or the United States.⁴³

And further:

Because of cabinet control over the drafting of legislation in parliamentary countries, even the [general] statutes are slanted in favour of discretionary secrecy.⁴⁴

In several fundamental senses, therefore — and this is a key point — the FoI statutes in nations without comparable systems of government to the United States seemed doomed before they were even introduced. By giving in to pressure to adopt the United States' model while trying to bend it and mould it to fit their own peculiar political inheritances and public service structures and cultures, nations such as Australia, Canada and the United Kingdom — all of which have Westminster heritages — have adopted systems of FoI that just do not sit comfortably with their political structures, which are prone to meddling by the government of the day and which do not work as effectively as they should in the public interest. Much the same can be said for Japan, Thailand, Mexico and every nation which has fallen under the spell of the United States' foreign policy push for FoI.

Finally, one can only wonder about the wisdom of the United States' policy of promoting its model as a global template for FoI when that nation's own governments and administrators seek to fight terrorism, not through leading by example in the areas of administrative openness and education, but through increased secrecy, reduced accountability and the emasculation of their own FoI statutes.

STEPHEN LAMBLE

Dr Stephen Lambie is Co-ordinator of Journalism in the Faculty of Arts and Social Sciences at the University of the Sunshine Coast.

References

1. Reno, Janet, 'Memorandum For Heads Of Departments And Agencies,' (1999) *FOIA Update*, Vol. XIX, No. 4: <http://www.usdoj.gov/oip/foia_updates/Vol_XIX_4/page3.htm> [Accessed December 17, 2002].
2. Ashcroft, John, 'Memorandum for Heads of all Federal Departments and Agencies,' (2001) *FOIA Post*: <<http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>> [Accessed December 17, 2002].
3. Murphy, Kathleen, 'War On Terror Restricts Information Flow,' *Stateline.org*, August 28, 2002: <<http://stateline.org/story.do?storyId=256975>> [Accessed December 17 2002].
4. 'OIP Gives FOIA Implementation Advice to Other Nations,' *FOIA Post*, December 12, 2002: <<http://www.usdoj.gov/oip/foiapost/2002foiapost30.htm>> [Accessed December 17, 2002].
5. Gerber, William and Lewis, Letitia, *Freedom of Information in American Policy and Practice*, Division of Policy Research, Office of Public Affairs, Department of State, 1948. Copy held by the Library of the University of Texas at Austin.
6. Gerber and Lewis, above, ref 5, p.ii.
7. DeFleur, Margaret, *The Development and Methodology of Computer-Assisted Investigative Reporting*. Dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Mass Communication in the Graduate School of Syracuse University, 1994. UMI Dissertation Services, Ann Arbor, Michigan, p.42.
8. Gerber and Lewis, above, ref 5, p.vi.
9. Gerber and Lewis, above, ref 5, p.7.
10. Gerber and Lewis, above, ref 5, pp.9,10.
11. Gerber and Lewis, above, ref 5, pp.23—26.
12. Gerber and Lewis, above, ref 5, p.28.
13. Gerber and Lewis, above, ref 5, p.30.
14. United Nations, history: <<http://www.un.org/aboutun/history.htm>> [Accessed 18 January 2002].
15. Gerber and Lewis, above, ref 5, p.46.
16. Gerber and Lewis, above, ref 5, p.33.
17. Gerber and Lewis, above, ref 5, p.34.
18. Mrs Roosevelt went on to become the inaugural Chair of the Human Rights Commission.

19. UN Commissioner for Human Rights: <<http://www.unhchr.ch/udhr/miscinfo/carta.htm>> [Accessed 18 January 2002].
20. Gerber and Lewis, above, ref 5, p.48.
21. Gerber and Lewis, above, ref 5, p.48.
22. Voice of America: <<http://www.encyclopedia.com/articlesnew/13542.html>> [Accessed 23 January 2002].
23. Gerber and Lewis, above, ref 5, p.51.
24. Gerber and Lewis, above, ref 5, p.51.
25. Gerber and Lewis, above, ref 5, p.51.
26. Mott, Frank, Luther, *American Journalism. A history: 1690-1960*, third edition, New York: Macmillan, 1962, p.861.
27. Singer, Michael, Jay, Chapter 12 'United States', in Rowat, Donald, C., *Administrative Secrecy in Developed Countries*, London: The Macmillan Press Ltd, 1979, p.312.
28. Relyea, Harold, 'Information Policy Around the World,' (1981) *Fol Update*, September. United States Department of Justice, Office of Information and Privacy: <http://www.usdoj.gov/oip/foia_updates/Vol_II_4/page7.htm> [Accessed 24 January 2002].
29. Relyea, above, ref 28.
30. Marsh, Norman, S. ed., *Public Access to Government-Held Information: a Comparative Symposium*, London: Stevens & Son Ltd., 1987, p.173.
31. Snell, Rick. 'The Kiwi paradox — a comparison of freedom of information in Australia and New Zealand', 2000: <<http://pandora.nla.gov.au/nph-arch/2000/Z2000-Oct-26/http://law.anu.edu.au/publications/flr/vol28no3/snell.htm>> [Accessed 20 September 2001].
32. Background to Fol in Australia: <<http://www.austlii.edu.au/au/other/alrc/publications/reports/77/ALRC77Ch3.html#ALRC77Ch3Introductio>> [Accessed 14 February 2002]
33. Snell, above, ref 31.
34. Background to Fol in Australia, above, ref 32.
35. Marsh, above, ref 30, p.174.
36. Background to Fol in Australia, above, ref 32.
37. Charter of the Organisation of American States: <<http://www.oas.org/juridico/english/charter.html#ch18>> [Accessed January 22, 2003].
38. Secretariat for Legal Affairs, Inter-American Convention Against Corruption: <<http://www.oas.org/juridico/english/sigs/b-58.html>> [Accessed January 21, 2003] and USAID/Colombia's anti-corruption program: <http://www.oas.org/juridico/spanish/col_res26.doc> [Accessed January 21, 2003]
39. Banisar, David, 'Freedom of Information and Access to Government Records Around the World', 2002: <<http://www.freedominfo.org/survey.htm>> [Accessed 21 July 2002].
40. The World Bank, 'About Us': <<http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/0,,pagePK:43912~piPK:36602,00.html>> [Accessed 21 July 2002].
41. International Monetary Fund, 'What is the International Monetary Fund?': <<http://www.imf.org/external/pubs/ft/exrp/what.htm#origins>> [Accessed 21 July 2002].
42. Rowat, Donald, C., *The Right to Know: Essays on Governmental Publicity and Public Access to Information*, third edition, Ottawa: Department of Political Science, Carleton University, 1981, pp.150 & 153.
43. Rowat, above, ref 42, p.157.
44. Rowat, above, ref 42, p.158.

The Freedom of Information Act 2000 and whistleblowers in the UK

Some reflections

Introduction

Much has been written on the background, history, and the various reasons why a country such as the UK should adopt both a Freedom of Information Act and new law to protect so called 'whistleblowers'. The rationale for a more transparent and open form of government, as well as a less corrupt public life and business world, are fairly evident to readers of this journal. This article does not seek to repeat such arguments, but instead will examine the relationships between these two areas of law, and their relationship with other legal, political and constitutional changes taking place in the UK today. It will seek to argue that while the two main pieces of legislation which we shall critically outline are now becoming clearer, it is perhaps the development of a culture that values openness which will bring about the most lasting change. In the words of one commentator (Cornford) have these legislative changes (referring to the Fol) been genuine or a sham?

The two main pieces of legislation which are relevant to our discussion are the *Public Interest Disclosure Act 1998* (henceforth PIDA) and the *Freedom of Information Act 2000* (henceforth FoIA). PIDA, which came into force in July 1999, has had a relatively brief life span. On the other hand, while some parts of the FoIA were introduced in November 2002, the Act and all the rights contained in it do not become fully applicable until January 2005. It is thus not yet possible at the time of writing to assess the

full impact of the PIDA in practice or how the FoIA may affect UK law and government. However, some material is available on PIDA and commentators have been able to make predictions which have been generally accepted as the likely outcomes of the FoIA development. Also, the long series of consultations, guidances and drafts of the required codes for FoIA give some indications as to the approach and impact that the new law may have on the UK.

Background to the discussion

Before we examine these two statutes it is worthwhile to reflect on the situation prior to their enactment and on the situation more widely since their passage. The transition from a traditional political culture in the UK that has had as one of its key values the requirement of almost total secrecy, to the current situation, is in many ways quite remarkable. This secrecy derived from numerous statutes, of which the most famous was the *Official Secrets Act 1911*, but also the ability to use the common law of Confidentiality to restrain the release of official information, as in the famous 'Spycatcher' litigation.¹ The law relating to public interest immunity allowed the state to withhold evidence during litigation, but since the Matrix Churchill case the practice of the state seems to be more restricted with judicial intervention to decide if the claim for such immunity is valid.

Earlier attempts at more open government arguably began with legislation such as the *Local Government (Access to Information) Act 1985* and the *Access to Medical Reports Act 1988*. Whilst flawed, these were an attempt in certain fields to allow some release of information. Slight reform of the *Official Secrets Act* in 1989 ended the very wide ambit of the former s.2 of the 1911 *Official Secrets Act* but at the same time removed the public interest defence. Other statutes allowing limited access to personal files and health records followed. In 1994, the government introduced a non legally binding Code of Practice on Access to Government Information which, though amended in 1997, is still in use and will continue until the FoIA is fully introduced. The *Local Government Act 2000* also has as one of its aims greater accountability for the actions of elected councillors and officials. The Act's new Standards Committees at local level, a national Standards Board and Ethical Standards Investigators³ indicate that major steps have been taken, at least in local government, to achieve a more transparent public service. If one includes the Nolan Committee with its influential reports, the register of MPs' interests and the seven Nolan Principles of Public Life,⁴ together with the Parliamentary Commissioner for Standards, it can be seen that some progress has been made even in central government.

The *Data Protection Act 1984* (DPA), largely succeeded by the Act of the same name in 1998, chimes well with these most recent set of developments. Although concerned with protecting the use and misuse of data kept on the individual, it did force government and business to reflect on why and how they keep and use such information. The role of the powerful Data Commissioner has provided an interesting model for the new FoIA, and indeed this later Act has combined the role of the Data Protection Commissioner with that of a similar body for the FoIA, and renamed them the Information Commissioner. This person, together with a new Information Tribunal, will have wide powers under the FoIA to which we will return below.

Essentially the DPA applies to personal information or data which is kept or processed automatically or, with some exceptions, manually. If such information or data is held, the holder must register with the Information Commissioner and comply with the data principles. A request about data kept on oneself will be dealt with under this Act. If the request for such data is from someone else, it is to be treated as a request under the FoIA, (s.40) but is likely to be exempt by the FoIA as concerning personal information, unless the public interest test is met. The complexity and overlap between these two areas of law have been criticised by a number of commentators. While some issues have been clarified others are still unclear.⁵

The other major legislative development which occurred after the Labour Party formed the new government in 1997 is also linked to our discussions. It concerns the *Human Rights Act 1998*. Implemented after a two-year delay, in October 2000, this statute affects how all UK law is to be interpreted and applied. All legislation must be read in the light of the Articles of the European Convention on Human Rights (ECHR) 1950 and the jurisprudence

developed under it over the last 50 years. It is also a requirement that all public authorities must act in a way which is not incompatible with the Convention, unless it is not possible to do so. This requirement will affect the work of all public authorities whose definition is quite wide and includes most importantly all courts and tribunals.⁶ This Act could well have important repercussions for the working of the two main statutes central to our discussion. In particular, the convention jurisprudence has not developed a specific general right to freedom of information, even under the most obvious provision, Article 10. This Article, which is concerned with freedom of expression does recognise the value of receiving information in order to develop the right of free expression. However, the European Court of Human Rights in Strasbourg, has refused to go further and to find a free standing right to information. In Article 10 and other rights such as Article 8, concerning the right to private and family life, the European Court has only been willing to recognise a right to access such information as is necessary to enjoy the rights such as are contained in Articles 10 and 8.⁷

Finally it is worth noting that moves have taken place at an international level which affect the working of the legislation in discussion here. In addition to the European Convention of Human Rights, the UN Economic Commission for Europe has developed the 1998 Aarhus Convention in relation to providing more information about environmental issues. This Convention is very explicit in its aims of wishing to expand access to such information as a necessity to developing greater participation in decision making. Further, the European Community (EC) has, as a signatory to the UN Convention, also developed principles of greater access to such environmental information, and the earlier directive in this field is to be updated by the forthcoming EC Directive in relation to Public Access to Environmental Information. The UK is currently having to redraft and update its 1992 Environmental Information Regulations to achieve greater flows of information in this area. The EC itself has been much criticised for the secrecy of its activities, and has finally developed, after much resistance, a policy and a new Regulation, 1049/2001. This is designed to provide greater access to information about and held by the three main institutions of the EC, ie the European Council, Commission and Parliament.

The Public Interest Disclosure Act 1998

The PIDA 1998 is an ambitious project to protect any worker in either the public or the private sector who reveals information about wrongdoing to others — internally or externally.⁸ It seeks to encourage a greater flow of information by trying to ensure that workers are not discriminated against or lose their jobs when reporting a concern about wrongdoing to the appropriate authorities or to the public or media generally, subject to certain quite strict procedural requirements. It should be noted that the Act only applies to workers including trainees, but does not apply to the self-employed, voluntary workers, the security services or the armed services. Protection is provided in the form of the ability to take the employer to an Employment Tribunal to claim compensation if the worker

suffers some detriment or the possibility of obtaining a court injunction to prevent the victimisation occurring. Only information that is provided relating to particular concerns are protected but they are quite general in nature. They include concerns about any crime, civil matters such as breaches of contract, miscarriages of justice, danger to the environment and health and safety and the attempts to cover up such activities. Thus the ambit of disclosures is quite wide.

Disclosures are dealt with differently depending on to whom they are made. If made internally, that is within the organisation, all that is required is a disclosure in good faith with a reasonable suspicion that the wrongdoing has occurred or is likely to occur. The same applies if any public sector worker gives the information to the main governmental department with whom they work or are contracted. If the disclosure is external to an appropriate or prescribed regulator, the same requirement of good faith is needed as well as a reasonable belief that the information is substantially true.

The situation does not improve when one looks at the protection that might be given to disclosures not to the above types of recipients, but to those most whistleblowers are likely to think of, namely the media, the police, members of parliament or non prescribed regulators. Here, the potential discloser, in addition to satisfying the requirements when making a disclosure to a prescribed regulator, has to show that the discloser acted in a way which is reasonable in all the circumstances, has not made the disclosure for personal gain and must pass further tests involving all of the following: that the person reasonably believed that victimisation would occur, that there was a reasonable belief that a cover up was likely and there was no prescribed regulator available or that the matter had been already raised internally or with the regulator.

It is clear that there are doubts as to the meaning of such phrases as 'good faith' and 'reasonable suspicion' or 'reasonable belief' in the legislation. There is some guidance on the meaning of reasonableness which includes the response of the regulator or the employer, the seriousness of the matter and whether any internal policy or procedure is available or was used first. The clear intention is to encourage the resolution of these concerns within the organisation through internal policies and systems, with external disclosures seen as a last resort. However, there is no legal requirement to have such policies or procedures.

The complexity of all these requirements has meant that the Act has perhaps not been used to the extent anticipated. The advisory and campaigning NGO, Public Concern at Work (PCAW), recently estimated that in the first three years of its existence up to July 2002, there had been 1200 claims under the Act, the largest award being of £805,000 for a company director who blew the whistle on a misleading company prospectus. A number of successful claims have involved the NHS where employees have gone to the press about failures in that service. A proportion of claims have failed however, and PCAW points out that it is increasingly difficult to assess how the Act is working. This is due to new employment tribunal

rules that allow settlements to be kept secret. As about 70% of all claims are settled before the hearing, the problem is obvious.⁹

Other concerns involve the lack of knowledge generally of the Act, its complexity, the burdens of proof imposed in order to gain protection and the lack of the remedy most desired by disclosers, which is to retain their jobs. As recently seen in the events surrounding Enron and WorldCom in the US, in the same way the value and need for legislation in the UK was recognised after a series of major disasters and cover ups. Employees in these situations were often the only ones and those best placed to know what was going wrong. However, they were prevented from raising their concerns from fear of the repercussions that would follow if they revealed such information. The passage of PIDA attempted to value and encourage this whistleblowing. The value of these disclosures to prevent or reveal such criminal activity has been recognised most recently in the UK by the new Financial Services Authority, the main regulator for all aspects of finance and investments. It issued a policy statement in April 2002 encouraging the use of PIDA, and has set up a telephone and an e-mail address for the use of such whistleblowers. It is to be noted that it strongly encourages such matters to be dealt with internally first, in accordance with the aims of PIDA.

Freedom of Information Act

As to the FoIA, again much has been written on this legislation¹⁰ and the detail will be left to those contributions. We will discuss only the main points of the Act. It should be noted that the FoIA only applies to England, Wales and Northern Ireland, as the Scottish Parliament passed its own Freedom of Information Act in April 2002. In addition to the Act, under s.45 there is a Code of Guidance required to be produced by the Lord Chancellor, and this was published in November 2002. There is also a requirement for each public authority to produce, under s.19, Publication Schemes to list proactively what they are providing under the Act to the public and how it might be accessed. Each such Scheme has to be approved by the Information Commissioner or to follow a model produced by him. This part of the Act, as we noted earlier, is being phased in over three years up to 2005, beginning with central government bodies from November 2002. It is of interest that the code requires under s.50 each authority to have an internal complaints system in place by the time of their Publication Scheme.

The main principles are contained in Part I of the Act. This makes it clear that there shall be, for the first time in all of the public sector (as opposed to such areas as local government mentioned above), a new legal right to request and receive information held by a public authority. There is a further right to be informed if there is such information and why, if exempt, it may not be communicated. This right in Part I is immediately qualified by a wide list of exemptions in Part II. The right of access may be exempt absolutely and partially either on a 'class' basis or on a 'contents' basis.¹¹

The FoIA is aimed primarily at public authorities, but their definition in the Act includes those acting on behalf

of public authorities or carrying out their duties under contract which may be designated by the Minister, under s.5, to be deemed as public authorities. This means that the Act has a wide potential. It has been estimated by the Lord Chancellors Advisory Group in July 2002 that in total about 88,000 such bodies may be caught by the Act. Examples of private bodies likely to be designated are the companies which carry out audit work on local and central government for the Audit Commission and the National Audit Office respectively.

Major concerns stem from the wide-ranging exemptions in Part II which in some circumstances are more restricted than the earlier non-binding Code. In addition to two exemptions which apply where the cost of retrieving the information is regarded as excessive in relation to the fees to be laid down (s.12) and an exemption where the requests for information are regarded as vexatious or repetitive (s.14), there are at least 30 other exemptions according to the Campaign for Freedom of Information. The types of exclusion are not so unusual in comparison with legislation in other countries, and include the usual catalogue of situations such as dealing with national security, defence, international relations, the economy, personal information and law enforcement. What appears to be different is the way in which a number of areas of information are absolutely exempt, such as, for example, s.23 relating to certain security services or information contained in court records under s.32. But s.41 excludes absolutely information received in confidence and s.21 excludes information reasonably accessible by other means. There is no need for the authority to do a balancing exercise in these circumstances.

Section 2 lists other categories which are 'qualified' exemptions with many of the categories of information becoming exempt if to allow disclosure (unless absolutely exempt above) in a certain 'class' of information 'the public interest in maintaining the exemption outweighs the public interest in disclosing the information'. If in a 'contents' based claim there would or would be likely to be prejudiced a specified interest in the relevant section of the Act, then again this information may be withheld. Note that the Act only requires 'prejudice', whereas the earlier White Paper in 1997 which was issued prior to the Act, required 'substantial prejudice' before exemption. This in practice makes a big difference, allowing far more exemptions.

Further criticism has focused on two controversial sections which were included. These centre on the exemption in s.35, in relation to the formulation of government policy except for statistical information. Section 36 allows an exemption where 'in the reasonable opinion of a qualified person' the release of such information would or would be likely to prejudice, amongst other things, the effective conduct of public affairs! The width of this exemption is extraordinary, and leaves in the hands of such a 'qualified person' the decision to release the information. It will be of no great surprise to find that such qualified persons are usually the relevant ministers!

Interestingly, the Act is retrospective and so applies to information being collected prior to 2005. Time limits are laid down in the Act, usually of 20 days, to respond to a

request, but this runs only from the payment of any appropriate fee. Time limits can also be extended where appeals take place. In addition to the need for prior approval of publication schemes by the Information Commissioner (IC) or the adoption of a model scheme, Part IV of the Act deals with the enforcement of obligations in Part I. Informal and local resolution of a dispute is encouraged by an internal complaints system of the public authority in the first instance. This is because the IC does not need to come to a decision under s.50 unless internal complaints are exhausted first. The IC can also issue one of a series of decision, enforcement and information notices, depending on the situation, requiring compliance with the Act under ss.50-52. Failure to comply with one of these notices can be treated as contempt of court. However, there are some limits to these powers. The first is that there is an appeal available under Part V to the Information Tribunal against one of these notices. This body can review all the circumstances and is able to override the decision of the IC and allow an appeal and or issue any notice that the IC could have issued. A further appeal on a point of law to the High Court can be made by either party.

A more controversial and much criticised restriction on the powers of the IC and Tribunal is the veto in s.53 whereby a minister, government department, or other authority designated by the Secretary of State may override the decision of the IC or the Tribunal. This can be done if the Secretary of State has formed the view on reasonable grounds that there has been no failure to comply with the Act! Such a view may be challenged but only by judicial review in the courts, and therefore means a great deal of power is retained by the government if it so wishes.

Some comparisons and contrasts

There follow some comments on interesting aspects of similarity and difference between these two pieces of legislation. Of necessity these are in general terms and in outline only.

The first and most obvious comparison is that the FoIA applies to 'public authorities' and they are listed in the Schedule to the Act. Although this term is widely drawn and private bodies carrying out public functions may be designated by the Minister it means this Act does not concern most private companies. The PIDA does cover all private bodies as well as public authorities, and although there are exclusions, it clearly has a wider ambit.

Secondly, only those who are 'workers' are protected under the PIDA, and so the self-employed and volunteers are not covered. Of more importance, PIDA is not available to those who work in the Security Services and the armed forces. In the same way, the FoIA exempts the work of the security services and others, either because they are not listed as public authorities or they are absolutely exempt in the Act.

Thirdly, PIDA raises concerns about the motives of the person who reveals information, linked to issues of 'good faith', and where for instance information is given to the media, the discloser has to show that it was not made for personal gain. The FoIA, on the other hand, is not

concerned with motives as no reasons have to be given for the request of the information. They may possibly arise indirectly though as part of the balancing exercise where applicable between the public interest in disclosure and that of maintaining the exemption or in examining possible prejudice.

Fourthly, both statutes either directly, as in FoIA, or indirectly as in PIDA, encourage the desirability of resolving issues internally, if at all possible, in the first instance. This is obviously to the benefit normally of all concerned as it avoids damaging publicity and litigation. The result though is that it does therefore make it more difficult to either appeal to the IC or to successfully bring a case in an employment tribunal.

Fifthly, enforcement differs substantially in that the FoIA builds on the experience of the Data Protection Commissioner and creates the new Information Commissioner to monitor and enforce the Act. The Tribunal and rights of appeal to the courts, together with proactive Publication Schemes, represent a quite extensive regulatory system. The PIDA by contrast and also perhaps by its very nature, leaves everything up to the individual to decide whether to go public and blow the whistle on wrongdoing. There is little if any support for such a person except for the NGO Public Concern at Work, or if the person is a member of a trade union or professional organisation it may assist.

Sixthly, remedies or outcomes are quite different. Breach of the FoIA or failure to obey notices by a public authority can result, unless exempted or overruled, in contempt of court with fines and imprisonment. The ultimate outcome is either receipt of the required information or its non disclosure by the authority due to some exemption or ministerial override. Note that there is normally also a duty to confirm or deny that the authority holds the requested information, and normally reasons have to be given for a decision to withhold the information. However, where exemptions are claimed by the authority, the authority may also refuse to confirm or deny the existence of the information, a regressive step in view of the aim of the Act. The PIDA is purely a civil matter between the individual and the employer, with the remedy of damages for proven victimisation and or loss of employment. In theory, the Employment Tribunal may order reinstatement but in practice this is likely to be rare.

The attitudes of the courts and tribunals are crucial in considering the workings of both statutes. It is still perhaps too early to assess how the courts are approaching the PIDA situation, and tribunal decisions are often not reported. In relation to the FoIA not only the courts, but the attitude and approach of the Information Commissioner will be of great importance in practice. It may be that the *Human Rights Act* which will apply to all public authorities, the IC and the Tribunal, as well as the courts themselves, could have some influence on the way in which they reach their decisions, As we have seen though, the jurisprudence derived from the European Convention has so far not proved very helpful generally in accessing information. It is possible information for certain purposes may be encouraged following the cases involving Article 8 and the others referred to above.

Finally, what is hopefully apparent is that both Acts impose a complex system on those revealing or requesting information. The difficulties of understanding the PIDA legislation as well as applying it mean that many are likely to have been dissuaded from considering a public interest disclosure. Although we are not yet able to assess the actual working of the FoIA, the different powers of intervention of the IC, the override of some decisions by ministers, the width and number of exemptions, the difficulty of giving meaning to terms such as prejudice and the balance of competing public interest issues, give some indication of how many problems are likely to arise.

Conclusions

As has been pointed out by Vaughn in this journal¹² in relation to the situation in the United States, even though 'most whistleblower statutes are independent provisions separate from freedom of information laws, they remain connected to freedom of information laws through the relationship of common principles and goals'. These common principles and goals are most clearly evident in relation to public sector workers, where there are clear concerns in relation to a transparent and accountable government. They are also clear in relation to the private sector recently where lack of information, secrecy and misinformation have led to major corporations suffering bankruptcy, as well as a more general loss of faith and trust in the accounts and public statements of corporations.

In other words, if the FoIA legislation were to work well in the public sector, there would be little need for whistleblowers and PIDA. However, PIDA is an attempt to allow greater access to information more generally where it is not possible to obtain such information as, for example, where the information is held by a private body or is exempt, or not requested as not known about under the FoIA. Such information may also not be available or controllable under data protection rules as the information may not concern personal information.

Perhaps, more controversially, it is time to start to consider whether some kind of access to information is necessary in the private sphere. Even with due regard for personal information and some protection of valuable commercial secrets there is much that could be done. Corporations are increasingly required to reveal large amounts of information for certain specified purposes such as relating to the environment. Why not continue and extend these requirements? So much of current government or public activity now takes place or is provided by private companies, that their influence is increasing tremendously. Some such activity may now be caught by the FoIA provisions if ministers are willing to designate them as such. The Act's weaknesses, however, illustrated above mean little real change is likely to occur even when the Act is fully implemented.

The argument for greater openness in the private as well as the public sector could be based on the increasing need for accountability of private corporations in our society. The recent allegations made against private corporations of corruption and theft, their impact on the environment, on workers' health and safety, on employment and generally of unlawful and misleading activities that affect investments

could all arguably be justifications. The privilege that the state has given to private corporations to use the limited liability corporation as a vehicle for investment, could perhaps demand in return that the corporation may be more open. The increasing calls for corporate social responsibility from social and public interest action groups, shareholder and pension groups, and the corporate world itself as well as from bodies such as Transparency International and the government would seem to suggest a growing recognition of the value of such openness.

In the meantime, if there is no adequate method of accessing knowledge legally under the FoIA provisions, we are going to have to rely on the goodwill of the government and public servants to operate the system in a more open way, as well as on the effectiveness of the Information Commissioner, the Tribunal and the courts. The *Human Rights Act* may assist depending on how it is applied and interpreted. So, perhaps, may developments from the EC with its increasing interest in issues of a more transparent approach to administration and in aspects of corporate social responsibility. In the meantime, in spite of all the difficulties they face, it seems we will have to continue to rely on those public-spirited citizens who are prepared to blow the whistle on wrongdoing that they encounter.

Unfortunately, the reality is that the legislation discussed here is unlikely to assist in the pursuit of a more open and accountable public government. The private sector is still, to date, relatively untouched. Even if the pieces of legislation discussed above were able to function as fully as originally intended, they provide no more than a useful development on the way to a regime designed to allow truer access and freedom of information. In the end, whichever legislation is developed it must go hand in

hand with a wider recognition in the public and private sector of the value of more open systems. As Birkinshaw¹³ has commented, unless 'there is a change in attitude and ethos in our public administration and in the public and private interface, FoIA by itself will be something of a confidence trick'. Or as Cornford¹⁴ has suggested in answer to his question posed at the beginning of this paper, the FoIA is closer to being a sham than to being a genuine development in the move to greater transparency and access to information in our society.

STEPHEN HOMEWOOD

Stephen Homewood is Principal Lecturer in Law, Law Academic Group, Middlesex University.

References

1. Cornford, T., 'The Freedom of Information Act 2000 — Genuine or a sham?' (2001) 3 *Web JCLI*.
2. Amongst the large number of cases, see *AG v Observer Newspapers*, (1986) and *AG v Guardian Newspapers* (1987).
3. Homewood, S., PIDA 1998 and Local Government, Unpublished paper at 1st International Whistleblowing Seminar, University of Indiana, April 2002.
4. See 1st Nolan Committee Report on Standards in Public Life, 1995 Cm. 2850
5. See Birkinshaw, P., *Freedom of Information*, 3rd edn, Butterworths, 2001, Chapter 7; Wadham, Griffiths and Rigby, *Blackstone's Guide to the FoIA 1998*, Blackstones Press, 2001, Chapter 10.
6. For the Act generally see Wadham and Mountfield, *Blackstones Guide to the Human Rights Act 1998*, 2nd edn, Blackstones Press, 1999.
7. See *Leander v Switzerland* 1987, 9 EHRR 433; *Guerra v Italy* 1998 26 EHRR 357 and generally 'Chapter 1 in Wadham, Griffiths and Rigby, above, ref 5.
8. For a wide overview of this Act from a variety of perspectives, see Lewis, D., (ed) *Whistleblowers at Work*, Athlone Press, London, 2000; Cripps, Y., *The Public Interest Disclosure Act 1998*, in 'Beatson, J. and Cripps, Y. (eds), *Freedom of Expression and Freedom of Information*, OUP, Oxford, '2000, pp.275-87.
9. See PCAW publication, (2002) 2 *The Whistleblower* and generally their website <www.pcaw.co.uk>.
10. See ref 5 above, and see also Austin, R., 'Freedom of Information; The constitutional impact', in Jowell and Oliver (eds), *The Changing Constitution*, 4th edn, OUP, Oxford, 2000.
11. See Wadham and others, chapter 6 and Birkinshaw, chapter 6 above at ref 5 on these categories and the 'definition of class and contents based exemptions.
12. Vaughn R., 'The Relationship between Freedom of Information and Whistleblower Protection', (2002) 99 *FoI Review* 29.
13. Birkinshaw, above, ref 5, p.482.
14. Cornford, above, ref 1, p.13.

To Subscribe!

Freedom of Information Review

\$66 (6 issues) per annum

At the time of subscribing you will be sent all issues for the current year.

Cheque enclosed (payable to LSB Cooperative Ltd) OR

Please charge Bankcard/Mastercard/Visa/Amex

No.

Signature

Card Expiry Date

Name

Address

.....

Send to: Legal Service Bulletin Co-operative Ltd, Law Faculty,
Monash University, Victoria, 3800, Tel: (03)9544 0974
Fax: (03)9905 5305 Email: m.gillespie@law.monash.edu.au

Editorial Co-ordinator: Elizabeth Boulton

Typesetting and Layout: Last Word

Printing: Thajo Printing Pty Ltd, 4 Yeovil Court, Wheelers Hill 3150

Subscriptions: \$66 a year or \$44 to *Alt. LJ* subscribers
(6 issues)

**Correspondence to Legal Service Bulletin Co-op.,
C/- Faculty of Law, Monash University, Clayton 3800**

Tel. (03) 9544 0974 email: L.boulton@law.monash.edu.au