out of breaches or evasions of the law. Further, whilst the applicant had expressed concern for the well being of himself and his family, that anxiety did not establish that there was anything other than a remote possibility of danger. Pepperell needed to show that the disclosure would or would be reasonably likely to cause danger — that there was a chance of such danger occurring which was 'real — not fanciful or remote'. (Referring to *Department of Agriculture and Rural Affairs v Binnie*, Supreme Court, 9 December 1988, unreported).

'Confidence'

In looking at s.35, the Tribunal then had to consider if the documents had been communicated in confidence. In determining whether the information in the letter was communicated in confidence the Tribunal had regard to the document itself, the nature of the information, the purpose for which and the circumstances in which it was provided, and the statement by the applicant that he intended the letter to be confidential. In this case the letter contained no express statement that it was communicated in confidence. It was only after its request for production under the *FoI Act* that the applicant alleged confidentiality. The Tribunal concluded that, having regard to the sensitive nature of the information, to the fact that the applicant, being a police officer, would have an awareness of the need for confidentiality, to the reasonable expectation that information of the kind would ordinarily be received and treated in confidence, and to the evidence of the applicant, the letter was communicated in confidence. However, while he accepted that the intention of the applicant was that the letter be confidential, confidentiality was limited only to those parts of the letter which were not in the public domain.

In order for s.35 to succeed the material not only has to be communicated in confidence but it also has to satisfy either para (a) or para (b). The applicant submitted that the disclosure of the information under the Act would be contrary to the public interest by reason that disclosure would be reasonably likely to impair the ability of an agency or a Minister to obtain similar information in the future (s.35(1)(b)). The Tribunal found that it had not been established that other people would not write to the respondent in the future setting out complaints and furnishing information of a similar kind. In fact it was not argued in the case. All that had been submitted was that disclosure would have a detrimental impact upon relations between the Police Department and the Ministry of Housing and Construction. Therefore Pepperell had not made out any of the grounds of exemption on which he had sought to rely. The AAT affirmed the decision of the Ministry and ordered that the material be released to Walden.

[K.R.]

OVERSEAS DEVELOPMENTS

11TH ANNUAL DATA COMMISSIONERS MEETING

Concerns about transborder transfer of personal information and other international issues, especially those connected with the European market, were the main focus of the 11th annual Data Commissioners Conference held this year in West Berlin from 29 August–1 September. With the passage in the past year of data protection/privacy laws in Australia, Japan, the Netherlands and the Republic of Ireland, this was a banner year for data protection. The result was an attendance of over 140 delegates, including data commissioners, their staff and observers from around the world.

The highlight of the three-day meeting was the announcement by a Hungarian delegate, Dr Pal Konyves-Toty of the Central Statistical Office in Budapest, that his country would be shortly enacting a freedom of information and data protection law (along the lines of the present legislation in Ontario and Quebec) with coverage of all sectors of Hungarian society. This represents the first time a member of a communist country from the Eastern Bloc addressed such a gathering and contemplated the enactment of a data protection law. This was taken as an historic event, well received in the meeting place, the Reichstag, the former German Parliament which straddles the wall separating West and East Berlin.

Commenting on why the Hungarian government has come to be the first Eastern Bloc country to take such a measure, Lonyves-Toth told the assembled delegates that 'among socialist countries Hungary was the first to publish official computer statistics, [issue] a decree on software copyright, and a decree concerning the protection of computer equipment against fire'.

A draft Bill combining FoI and data protection has already been approved by the Minister of Justice, who submitted it to the Council of Ministers last January, where it was subsequently approved. The new proposed Hungarian Constitution also recognises every citizen's 'right to the protection of personal data' and, under the subsection on 'Liberties', it states that 'The Constitution among liberties has to acknowledge everybody's right to access information of public interest'.

When the Bill will actually become law was not made clear. Another Hungarian, Professor Dr Laszlo Solyom, architect of the proposed Bill, in a paper submitted to the conference, wrote of the problems they were grappling with in attempting to implement data protection principles and said he hoped to learn from the Berlin conference in order to resolve some of their difficulties. Konyves-Toty also announced that Hungary plans to become a signatory to the Council of Europe's Convention on Data Protection, since their proposed Bill contains the fundamental principles found in the Convention.

Another surprise announcement made during the proceedings was that the United Nations has developed 'Guidelines Concerning Computerised Personal Data Files' which outline the minimum guarantees to be incorporated into national legislation The Guidelines, expected to be passed by the UN General Assembly later this month, were proposed largely at the urging of a former member of France's data protection agency, the Commission on National Liberties (CNIL), Louis Joinet, currently serving in the Office of the French Prime Minister.

Canadian Federal Privacy Commissioner John Grace, addressing the delegates on the merits and the

perceived shortcomings of the proposed guidelines, praised the initiative of the UN in putting forth such a measure. The introduction and passage of the Guidelines is a reflection of the degree to which privacy/data protection concerns are growing in international bodies. Grace told the delegates that it was unfortunate that it was not widely known that the UN had developed such Guidelines. Though the General Assembly is about to adopt the Guidelines, Grace said that there was no guarantee they would be adopted by member countries. It is uncertain, he observed, to what extent these will be enthusiastically accepted within countries which currently do not have data protection and privacy laws for both the public and private sectors as 'even during the consultative process countries such as the US and Canada felt that the passage of the resolution should be delayed'.

One perceived weakness of the Guidelines is that the method of implementation of them would vary from country to country. On the positive side, they do not attempt to define privacy since the definition varies distinctly from country to country. So in this respect, said Grace, it is good that they articulated general principles of data protection and privacy.

The Guidelines propose criminal sanctions as a remedy for violations of any of the principles, which cover both the public and private sectors, but do not specify what these remedies should be, instead leaving it up to the legal regime in the country concerned. Grace objected to section 6 of the Guidelines, the power to make exceptions to the application of the data protection principles, as being too broad. The Guidelines state that departures from the basic principles: lawfulness and fairness, accuracy, purpose-specification, the right of access and principle of non-discrimination, 'may be authorised only if they are necessary to protect national security, public order, health and morality or the rights and freedoms of others, including persons being persecuted, and are specified in a law or equivalent regulation promulgated in accordance within the internal legal system which expressly states their limits and sets forth appropriate safeguards'.

Grace said that he hoped that the idea of 'national legislation restricting access to medical files on grounds of public health' would not be taken seriously.

Apart from some perceived problems and weaknesses of the UN proposal, he said that the important thing is that as data commissioners 'we should take the opportunity to adopt the Guidelines as it is good to have rules of the road for privacy which they can all follow'. 'Hopefully', he told the conference, 'this will now take the privacy message around the world'.

One of the primary differences of opinion among those participating at the conference was how other countries will be encouraged to develop data protection principles and ways in which a system will be developed to adequately protect the transfer of personal information between countries. One problem in trying to use the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is that it is perceived as a European instrument although it is open to signature by any country. The other problem is the means to develop protection for the transfer of data. The recent study on new technologies by the Council of Europe's Committee of Experts on Data Protection suggested that current data protection laws are sufficient to ensure the integrity of personal data being sent abroad. Some commissioners argue that an international body is required to develop rules and policies, whereas others prefer policy developments by the commissioners to handle the situation.

TOM RILEY

Article reproduced from Access Reports, published by Access Reports Inc., 6 September 1989.

RECENT DEVELOPMENTS

NEW SOUTH WALES *FREEDOM OF INFORMATION ACT*:

AN OVERVIEW

Freedom of information legislation has finally become a reality in NSW after a long history which began in 1977 when Professor Peter Wilenski recommended in a report commissioned by the Wran Labor Government entitled 'Directions for Change' that the time had come in NSW to begin the process of providing greater access to citizens of government information. Despite the Government's platitudes about being committed to open government no FoI legislation was passed in NSW. State administration remained clothed in secrecy.

FoI legislation was a 1987 campaign promise by the Liberal Party. After winning office the new Government introduced the first Bill on 2 June 1988. After amendments, the *Freedom of Information Act* was assented to on 21 March 1989 to become effective on 1 July, 1989.

Like the Commonwealth and Victorian legislation it gives the public the legal right to information held by State government agencies and public bodies. Unlike the Victorian legislation, the NSW Act extends to local and municipal councils but only in respect of files to an applicant's personal affairs.

The exemptions

Schedule 1 lists three categories of documents which are exempt. Part I consists of 'restricted documents'. These comprise Cabinet and Executive Council Documents; documents containing information exempt under Commonwealth or Victorian FoI legislation; and documents concerning law enforcement and public safety. The Premier of NSW, as the Minister responsible for FoI, may issue a conclusive certificate that a document in this Part is restricted. Such a ministerial certificate lasts for two years unless it is withdrawn sooner; it may be renewed.

For a second group of documents listed in Schedule 1 consultation is required between the agency and the affected third person before the decision is made to release them. These are documents affecting the personal affairs or business affairs of another, intergovernmental relations and the conduct of research.

Part 3 of Schedule 1 comprises a long list of other documents that may be exempt. They are internal working documents — those that would disclose the decision-making functions of the Government, a Minister or an agency and would be contrary to the public interest; documents subject to legal professional privilege; those relating to judicial functions of a court or