DATA PROTECTION NEWS FROM AROUND THE WORLD

1. International organizations

Council of Europe: On January 18th, the Committee of Ministers adopted a Recommendation (89) 2 on the Protection of Personal Data used for Employment Purposes (PL&B May '88 p.2 and August '88 p.2). It is the 6th sectoral recommendation which applies the principles of the Council of Europe Convention to a specific sector, like previous Recommendations on personal data and direct marketing, medical records and police records.

The Recommendation on Employment Data covers issues including:

* Data quality - data should be collected fairly and lawfully,
  - the purpose of collecting the data should be specified
* Individual rights - there should be a limitation on the quantity of data collected, and the time for which it is stored
* Collective rights - there is a need to consult with workers, or apply co-determination rights when data is collected
* Scope - the breadth of the Recommendation's application is illustrated by reference to:
  - access controls (see Norway's data security proposals p.22)
  - telephone logging (PL&B February '88 p.18)
  - audio-visual monitoring
  - automated personnel systems (PL&B February '87 p.11)
  - genetic and AIDS screening (see Canada's AIDS data report p.4)

The Recommendation covers automated records and manual records to the extent that they are closely related to an automated system.

Ireland has reserved the right to:

* apply the Recommendation only to automated files, and to
* exclude small family businesses from the Recommendation where members of the family are the only data subjects.

After meeting five times, the working party on the banking sector (PL&B August '88 p.2) has drawn up a draft recommendation which is due to be discussed by the Committee of Experts on Data Protection in the second week of March.

There have been meetings of a joint working party of the Committee of Experts on Data Protection and the Ad-hoc Committee of Experts on Bio-Ethics to discuss the collection and use of genetic data.

2. Countries with data protection laws

Australia: The Privacy Act 1988 (PL&B November '88 p.18) came into force on January 1st 1989. Privacy Commissioner Kevin O'Connor took office on this date. He was formerly Deputy Secretary of Victoria's Attorney-General's Department, and previously has worked as a barrister (advocate) and served on Australia's Law Reform Commmission when it was studying privacy issues in the early 1980's.

He currently has a staff of five and aims to have a staff of ten later this year. Graham Greenleaf, who wrote the PL&B report on Australia's new law, is the Privacy Commissioner's Special Advisor on Data Protection Policy. The Commissioner's office has been established in Sydney, Australia's largest city, and close to Australia's Human Rights and Equal Opportunities Commmission, rather than the relatively small capital city, Canberra.

His address is: Mr. Kevin O'Connor, Privacy Commissioner, Level 24, American Express Tower, King Street, Sydney, 20001, New South Wales, Australia. Telephone (02)-229-7600.

Canada: The Justice Department has recommended that the Privacy Act's extension to Crown Corporations should not apply fully to Air Canada and Petro-Canada (PL&B November '88 p.3). This decision, against the wishes of Privacy Commissioner, John Grace, was taken in response to the companies' claims that making them subject to the Privacy Act would damage their competitive position in relation to private sector companies in their markets. So far, there has been no announcement of how, in practice, this competitive harm would occur. Air Canada has an additional argument that it is now a mixed joint enterprise corporation, as the government owns 55% rather than 100% of the airline.

The Privacy Commissioner set a clear precedent on January 17th when he urged the Canadian Radio-Television Telecommunication Commission (CRTC) to prohibit Bell Canada (the telephone company) from providing its telephone subscribers' names, addresses and telephone numbers in computerized form to the direct marketing industry. The case illustrates the problems of Canadian, Australian and US law applying to federal government agencies but not to the private sector, as in Europe (PL&B November '88 p.24). The CRTC is bound by the Privacy Act but Bell Canada and its telephone directory supplier subsidiary, Tele-direct, are not.

To fulfill its function of supplying telephone directories, Bell Canada supplies lists of subscribers to Tele-direct in machine readable form for printing into directories. The question was raised whether these subscriber details were confidential or whether such lists could be sold for integrating or overlaying with other lists, for example, of subscribers' income, language, religion, type of dwelling, marital status and number of children. The Privacy Commissioner states in his formal submission to the CRTC, "While it may not be necessary to consider such information as confidential when contained in paper listings, it may be prudent to do so when contained in machine-readable form...We should bear in mind that such a "monitoring" and "tracking" tool would not be of interest to marketeers but, as well, to criminals and law enforcement agencies alike." To give substance

to his recommendation, the Privacy Commissioner stated that if the CRTC permits Bell Canada to offer a machine readable listing of its subscribers, against his advice, that it should impose a number of conditions, like:

* informed consent;
* no financial penalty for refusing consent;
* banning the release of additional information; and
* making publicly available a list of those who have bought such machine-readable data.

The full text of this recommendation is available from Privacy Laws & Business.

The use of the Social Insurance Number (SIN) as an employee identifier in federal government agencies will be restricted to examples specified in the law, the Canadian government announced in June 1988. On January 16th this year, the Treasury Board of Canada stated that it would develop and implement a new employee identification system to replace the SIN by April 1st 1991. This is part of the government's commitment that the SIN must be prevented from becoming a universal personal identifier. At an estimated cost of C$16 million, the federal government is reducing the SIN and related matching of computer files. SIN is being reserved for 22 statutory and mandatory social programmes for which it was originally intended.

John Grace, Canada's Privacy Commissioner, in a speech to the American Society of Access Professionals in September 15th last year explained the government's next step. "While the federal government has undertaken to put its own house in order first, it has also committed itself to ensuring the control of the SIN by provincial governments and the private sector. Notice has been given by the government that if voluntary action is not taken to prevent the widespread use of the SIN, federal legislative power, including the criminal law, will be used to ensure compliance."

In March, the Privacy Commissioner is due to issue a recommendation for a federal policy on data on the treatment of AIDS (Acquired Immune Deficiency Syndrome) patients. Although the federal government is not responsible for community health care nor for hospitals, it does govern a number of organizations which collect and hold health records, for example, the armed forces; Health and Welfare Canada which conducts medical examinations of federal employees; Veterans' Affairs Canada; Employment and Immigration Canada; applications for longterm disability benefit; and Correctional Service Canada responsible for prisoners.

The Commissioner's recommendations, which may well have influence at the provincial and municipal levels of government, have the aim of balancing the protection of individual rights and the protection of public health. His office has identified a number of public policy questions which apply equally to any country:

* Although the government's collection, use and disclosure of AIDS-related data should comply with the Privacy Act, should it be treated any differently from personal information about other communicable diseases?

* Does the Privacy Act prohibit or restrict manadatory AIDS testing?

* To what uses may AIDS-related information be put, to whom may it be disclosed and for what purposes?

Finland: will become the 23rd member of the Council of Europe on May 5th 1989, the 40th anniversary of the organization's foundation. Finland has declared its intention to sign and ratify the Council of Europe Convention on Data Protection.

Germany: Several amendments to the federal Data Protection Act are currently being discussed in the federal legislature. They include:

* introducing absolute liability for damages caused by data processed in an illegal manner or when consent of the data subject has not been given;

* restricting the law to automated records; and

* making the appointment of the federal Data Protection Commissioner dependent on a decision of the government rather than the legislature, as is the current practice.

Ireland: The Data Protection Act comes fully into force on April 19th (see p.10 and PL&B November '87 p.6, May '88 p.17, August '88 p.6 and November '88 p.6). Any companies needing to register should have done so by this date. All organizations operating in Ireland should obtain from the Data Protection Commissioner, in addition to the Act itself:

* The Guide to the Data Protection Act 1988

* Applications for Registration Guidance Notes

* The registration forms

His address is: Mr. Donal C. Linehan, Data Protection Commissioner, 74, St. Stephen's Green, Dublin 2, The Republic of Ireland. Telephone: (01) 789304

Netherlands: The Data Protection Act was adopted by the Upper House of the States General (legislature) on December 27th 1988 (PL&B November '88 p.11). The text adopted was the same as that adopted by the Lower House on September 8th 1987. The Act received royal assent on December 28th 1988 and was published in the Bulletin of Acts, Orders and Decrees on January 5th 1989. It will enter into force on July 1st 1989.

The first chairman of the Registration Chamber (the data protection authority) is Mr. K. de Vries, formerly President of the Administrative Court in Utrecht. He was appointed in early February.

Norway: List broking and direct marketing were top of the list of complaints to the Datatilsynet (the Data Inspectorate) in 1987, the latest year for which statistics are available. This is 15% up on 1986. It is significant that 1987 was the year when amendments to Norway's Personal Data Registers Act came into force, some of which tightened up the law on direct marketing and telemarketing (PL&B August 1987 p.5). These new amendments to section 8, (which passed on June 12th 1987 and came into force on July 1st and October 1st that year), were drawn up partly in response to media coverage which had raised public awareness, and at the same time had the effect of creating further publicity.

The Data Inspectorate received 25% more applications for permission to establish personal data registers in 1987 than 1986. The DI thinks that this increase is mainly due to more publicity about the law and more use of personal computers.

Less than 1% (5 out of 600) applications for permission to hold personal data registers were refused in 1987. The DI's retiring director, influential Helge Seip, explains to PL&B readers the reasons for the DI's turning down these applications. Although these refusals are clearly very few, the basis for these decisions will help companies prepare their applications and learn the limits of what is permitted in Norway.

* Three of the refusals were research projects where the collection of data was in conflict with professional secrecy rules.

* The fourth case was an application to keep automated files of car registration numbers in visitors' car parks to check them against the registration numbers of tenants' cars. The purpose of the database was to reduce the tenants' use of visitors' car parks. However, the DI ruled that this purpose did not outweigh the data protection interests of the visitors.

* The fifth case illustrates Norway's data protection law's coverage of both physical and legal persons. A market research and telemarketing company had collected data about computers used in 5,000 Norwegian companies. The applicant wanted to use this information for sale to potential suppliers of computer hardware and software and to telemarketing companies. The Data Inspectorate considered that the database increased the risk of revealing company secrets and personal data and increased the vulnerability of the companies. The applicant did not appeal against the DI decision.

Access control systems to places of work and other property are now common throughout Europe. They have featured on the list of the five subjects most frequently raised with CNIL, France's data protection authority (PL&B February '87 p.11). Now Norway's Data Inspectorate has drawn up a set of conditions for name-linked data files related to access control systems:

* Files on card holders and files on those authorized to gain access to different parts of a site may be established either following agreement between management and staff, or following permission from the Data Inspectorate.

* Permission from the Data Inspectorate is always needed for establishing a file on the movements of employees.

* The only acceptable basis for collecting data on the movement of employees is a security need, for example, a risk of industrial espionage. Therefore, it is essential to distinguish between access control data needed for security purposes and time-keeping data needed for administrative or management purposes.

* The usual time limit for keeping data on movement of employees is three months, after which the data must be deleted.

* The DI stresses that users or owners of access control systems should evaluate their own security needs rather than rely on assessments made by the people selling the equipment. The DI explains that it has seen a tendency for them to create needs for excessive systems.

Sweden: During last year, there were two cases which confirmed the Data Inspectorate's interpretation of the Direct Marketing Regulations. These Regulations, which came into force on March 1st 1988, impose a general ban on telephone marketing to private telephone numbers (PL&B February '88 p.16). In both cases, newspapers asked the Data Inspectorate for permission to collect private telephone numbers and use them for telephone marketing. The government supported the Data Inspectorate's refusal to allow them to do so.

By July 1st 1988, 27,000 file keepers were registered with the Data Inspectorate. In the year up to this date, there had been around 2,500 applications for the more complex permission to keep sensitive data; data on persons without direct links with the responsible file keeper, for example, membership, employment, or customers; and personal data obtained from any other personal file. During the same period, the Data Inspectorate received and dealt with 552 complaints from the public, mostly about debt collecting and consumer credit information.

The Data Inspectorate has drawn up general regulations and advice where data owners face common problems in interpreting the law for sectors like direct marketing (a simplified procedure for dealing with applications for setting up temporary files), data security, research, tax auditing, and the recording of personal data in local and regional government.

The legislature has passed a first resolution to add a provision to the Constitution giving the individual privacy protection when automated data processing is used.

United Kingdom: The Data Protection Registrar is currently working closely with the direct marketing and consumer credit industries to modify their practices on the fair obtaining of data and the ways in which they obtain information from third parties. It is in the detail of these

negotiations that the framework of legislation modifies the way in which these industries operate. This update concentrates on the direct marketing negotiations.

The Data Protection Registrar's Guidance Note 19, Fair Obtaining - Notification, issued in August 1988, has caused considerable tension between the Registrar's office and the direct marketing industry. The industry felt particularly threatened as the guidance note was issued around the time when the Registrar made his first enforcement order against a company which failed to remove a name from a list when requested to do so by a data subject. The industry has several objections:

* The industry was, firstly, disturbed by the tone of the guidance note which defined whether information is obtained fairly or not "as a question of fact for the Registrar in the first instance and subsequently for the Data Protection Tribunal in the case of an appeal."

* This upset the industry's assumption that its own Advertising Association's Code of Practice Covering the Use of Personal Data for Advertising and Direct Marketing Purposes, published with the support of the Registrar in April 1987 (PL&B August 1987 p.13), was generally a sufficient basis for conducting its business.

* The standards in the guidance note are strict. "The test of fairness is an objective one. It is results, not intention orientated. That the data user may not have intended to be unfair is not relevant to the question of fairness."

* The guidance note undermined the code's reliance on the public Data Protection Register as "the primary source of reference for data subjects about data users" (section 3.1.5). The guidance note states by contrast, "Individuals are not deemed to know the contents of the Data Protection Register. Generally, therefore, a reference to a data user's register entry will not be sufficient notification to meet the requirement for fair obtaining."

Although the industry's reaction was firstly uniformly hostile and alarmed, gradually, some companies within the industry pressed their colleagues for a dialogue with the Registrar, as straight opposition was unlikely to be worthwhile. As a result, industry representatives met with the Registrar in December and February. They explained the main ways in which the industry collected information and the problems of applying strict principles of fair collection. The Registrar held firm to the main lines but agreed that the appendix to the guidance note was not clear enough, needed to be revised and that he would submit any new version to the Advertising Association for consultation.

Privacy Laws & Business will monitor these developments. They provide an interesting example of how an industry needs great skill in working in a legal environment of self-regulatory guidelines within a framework of law.

United States of America: The Computer Matching and Privacy Protection Act was signed by the President on October 18th 1988 and is due to enter into force nine months after that date in June this year. It covers

federal agencies and requires them to follow certain standards when carrying out computer matching to ensure that individuals are not harmed by unauthorised use of name-linked information or refused government benefits because of inaccurate data. The main provisions are that:

* individuals should be informed when they are the subject of a data match;

* individuals have a right to give their views of the facts;

* each federal agency intending to carry out a computer match should create a data integrity board to review the process; and

* each computer match programme should first be subject to a cost-benefit analysis.

The Video Protection Act was passed by Congress on October 19th 1988. Its purpose is to prevent the rental or sale of names and addresses of people who have rented videos linked to the names of the videos.

This is a clear example of where the United States retains its approach of tackling certain sectors, if a sufficient problem exists. The protection of privacy achieves greater importance with this law than mere accurate and efficient record-keeping. However, the problem with this approach is that similar sectors with similar problems are excluded in order to achieve success with a narrow measure. In this case, an effort to ban the sale or rental of lists of names and addresses of individuals identifying which books they have borrowed from a library was defeated.

3. Countries planning data protection laws/rules

Greece: A revised Data Protection Bill (PL&B May '87 p.6 and February '88 p.6) is expected to be put before the legislature shortly. It takes into account several of the suggestions made at the Council of Europe conference held in Athens in autumn 1987 (PL&B February 1988 p.7). However, it is uncertain whether the bill will make much progress before the elections, due by June this year at the latest.

Hong Kong: The government has begun a review of the way in which its Data Protection Principles and Guidelines (PL&B May '88 pp.7 and 14), published in March 1988, have been implemented. Nearly 4,000 public and private sector computer users in Hong Kong were sent the document last year. The review is likely to take a few months and the main question to be resolved is whether Hong Kong should move to a data protection law, and if so, in what form. The review will take into account computer users' views.

Spain: Last summer, the socialist/communist group in the Cortes (legislature), the Izquierda Unida, put a motion to the government urging it to make progress on its data protection bill submitted to the Cortes in 1985. So far, the government has not responded.