

## REVIEWS OF DATA PROTECTION AUTHORITY ANNUAL REPORTS

### Ireland's Data Protection Commissioner's Annual Report 1993

The Fifth Annual Report 1993 of Ireland's Data Protection Commissioner gives an overview of the supervising and monitoring activities of the Office of the Data Protection Commissioner.

This is the first annual report to be prepared by Commissioner, Fergus Glavey, who was appointed in September 1993. He covers:

- raising awareness, for example, "awareness weeks" in different towns which included public lectures, radio and television interviews, leaflet and poster distribution and the establishment of information stands in main shopping malls; the launch of a public survey on public perceptions about data protection; and promoting awareness of the law to data controllers,
- dealing with enquiries (about 50% of enquiries were about credit information) and complaints (24 formal complaints in 1993 against both public and private sectors),
- registration (he warns of stronger enforcement action against those who refuse to register),
- the expectation of codes of practice to cover direct marketing, insurance and credit information.

The report also includes a section on international developments, namely the EU Data Protection and ISDN Directives and inter-governmental conventions in the area of police, customs and judiciary co-operation.

In the second part of the Report, the Commissioner discusses on-going policy issues, in particular:

- the refusal by the Revenue Commissioners to grant a right of access by an individual to data on himself on the grounds that the

giving of such access would prejudice the collection of tax revenue,

- pressure to extend the use of an individual's Revenue and Social Insurance (RSI) number for other purposes and the rules which should apply to the transfer, access and matching of personal data between one government department/agency and another, and
- his views on the future shape of data protection and related legislation.

He sums up his view of the law which is "the belief that the individual's rights lie at the heart of our data protection system and should be a significant factor in evaluating the weight to be given to any competing rights which may arise."

**Fifth Annual Report of the Data Protection Commissioner 1993. No charge. Available from: The Office of Data Protection Commissioner, Block 4, Irish Life Centre, Dublin 1, Ireland.**

**Tel: + (353) 1 874 8544**

**Fax: + (353) 1 874 5405**

### Canada's Privacy Commissioner's Annual Report 1993-94

Nothing less than broad privacy legislation - for both government and business - will ensure Canadians hang on to their privacy in the face of the information highway. This is the main message in Canada's Privacy Commissioner's Annual Report 1993-94. "Without some rules, the first roadkill...will be our privacy and dignity...No longer is it sufficient to talk about protection privacy with sectoral codes, self-regulation, patchwork legislation and industry watchdogs," warns Bruce Phillips, Canada's Privacy Commissioner and urges nation-wide privacy protection rules for both public and private sectors.

Consumers are finding financial institutions monitoring their cheques; video stores pressing them for family income; and a long distance telephone service demanding their tax number. New information systems also promise consumer banking, shopping and government and medical services from home. These

systems will collect and record not just individual transactions but the patterns of those transactions. "Without any rules - and there are no rules in the private sector, except in Québec - Canadians could find their behaviour monitored and data manipulated, used and sold for purposes they neither envisaged nor intended."

The report refers to sectoral codes, in particular:

- the Canadian Direct Marketing Association's Code ("While it lacks an independent arbitrator to handle complaints, it restores considerable control to those who want to stop the mail and marketing calls."),
- The Telecommunications Privacy Protection agency ("appears to have been stillborn."),
- The Canadian Standards Association's continuing work on drafting a model private sector code,
- The Canadian Bankers Association code (and those of the individual banks) do not cover subjective information about individual clients nor do they protect bank employees. "broad disclosures are allowed to serve the banks' business interest.... And the codes will do nothing to prevent banks exchanging clients' personal information with the insurance companies and stock brokerages they may now own...."

"Each of these privacy solutions addresses only part of the problem. New communications networks will be shared by governments, most of which live by privacy codes, and private sector, most of which is unregulated."

The report lists some "privacy considerations that need explicit recognition on the Information Highway.

- Set out in law a fair information practices code to govern the highway,
- Give individuals control over the personal details that are transmitted on the highway,
- Assure individuals that the information will go when and where it is intended - the

confidentiality of electronic communications must be protected,

- Limit the collection of personal information to the details essential to providing the service,
- Do not disclose personal information without the individual's explicit consent, and explain data collection practices to clients,
- Protect transactional data (the record of how and when individuals use the system.) Do not gather and use transaction patterns for other purposes without the individual's consent,
- Develop cryptography and other technical and security measures to protect the privacy of electronic communications,
- Do not charge for privacy protection,
- Government must accept an oversight role to monitor privacy protection on the highway".

The Commissioner in his Annual Report also discusses several other trends and issues, such as data matching, ID cards, health records and smart cards. This section of the report covers the creation of a federal government Blueprint for an integrated electronic system to deliver its information services. "Not only would federal agencies create and manage shared personal databases, the Blueprint also envisages sharing the information with provincial governments and the private sector (which, except in Québec, has no built in privacy protections)....How will governments reconcile sharing personal databases with that fundamental privacy tenet - collecting only the minimum personal details needed to administer a program? There follows a number of specific privacy questions and the section concludes with the observation that "shared personal databases threaten becoming the single government computer file that privacy laws were enacted to prevent."

During the year, the Privacy Commissioner's office also:

- received 1,290 new complaints and found just under 40% were well-founded,

- handled 8,688 inquiries and publication requests, and
- carried out seven departmental audits, 13 follow-up reviews of earlier audits and 12 incidents of lost or improperly disclosed personal information.

**Annual Report 1993-94, Available from:**  
**Privacy Commissioner of Canada, 112 Kent Street, Ottawa, Ontario K1A 1H3, Canada.**  
**No charge. This publication is also available on audio cassette.**

**Tel: + (1) 613 995 2410**  
**Fax: + (1) 613 995 1501**

**British Columbia's Information & Privacy Commissioner's Annual Report 1993/94**

David Flaherty, the Information & Privacy Commissioner (IPC) for the Canadian province of British Columbia (BC), has published his first Annual Report 1993/94. The Freedom of Information and Protection of Privacy Act was proclaimed on October 1993, but David Flaherty was appointed as British Columbia's first IPC in July, 1993. The law covers all BC government ministries, and over 200 provincial government corporations, boards, commissions, and agencies.

The report mentions special features of the Act which have received favourable comment which include:

1. the strong statement of information rights and the duty of government to assist applicants requesting records,
2. the powers given to the BC IPC to ensure that government meets its responsibilities under the legislation, particularly the Commissioner's powers to order cessation of inappropriate personal data collection and disclosure,
3. the publication of a public records index which will list those government records which are available without a request for access under the Act,
4. the fact that harm must be demonstrated before information can be

withheld under the freedom of information part of the law,

5. the limitation of exceptions or assignments of time limits on exceptions,
6. a strong and usable public interest override which applies to all exceptions and can be used even without a request;
7. protection against the use of personal information for mailing lists or solicitations by telephone or other means.

The Annual Report provides the background to the Act and explains the role of the Commissioner and the mandate of his Office (see box on next page). It also contains summaries of selected reviews and complaints. Since the enactment of the Act, the Information and Privacy Commissioner's Office has opened 275 cases. The majority of these cases were closed through mediation and only six were referred to the Commissioner for an inquiry.

In October, 1994, the Act was extended to include local public bodies, such as municipalities, schools and school boards, local police forces, health care providers, colleges and universities. In the spring of 1995, the law will apply to the self-governing professions.

**BC IPC's Annual Report 1993-94.**  
**Available from: Crown Publications,**  
**521, Fort Street, Victoria, British Columbia,**  
**B8W 1E7, Canada.**  
**Price C\$4. Stock no. 813-4.**  
**Tel: + (1) 604 386 4636**  
**Fax: + (1) 604 386 0221**

**Manitoba's Ombudsman's Annual Report 1993**

*Privacy Laws & Business* has received the 1993 Annual Report of the Ombudsman of the Canadian province of Manitoba. The province's Freedom of Information Act was passed in July, 1985 and provides for a general right of access to records in the custody or control of a government department or agency. The Act mentions the protection of personal

privacy as an exemption to disclosure and does not regulate the responsibilities associated with collection, storage and use of personal data.

The weakness of Manitoba's law regarding privacy has recently become apparent. The contract for the computerization of health records was won by a company owned by a

bank which is subject to no privacy law in Manitoba.

**Available from: Ombudsman Manitoba,  
750-500 Portage Avenue, Winnipeg,  
Manitoba, Canada.**

**Tel: + (1) 204 786 6483**

**Fax: + (1) 204 942 7803**

#### WHAT IS PRIVACY?

David Flaherty, British Columbia Commissioner explains the meaning of privacy. His "sense of the particular privacy interests of individuals in information about themselves includes the following considerations:

- the right to individual autonomy
- the right to be left alone
- the right to a private life
- the right to control information about oneself
- the right to limit accessibility
- the right of exclusive control of access to private realms
- the right to minimize intrusiveness
- the right to expect confidentiality
- the right to enjoy solitude
- the right to enjoy intimacy
- the right to enjoy anonymity
- the right to enjoy reserve
- the right to secrecy.

With respect to specific data protection principles and practices for government personal information systems, the following list incorporates the main considerations and values that my colleagues and I are trying to promote in British Columbia:

1. The principles of publicity and transparency (openness) concerning government personal information systems (no secret data banks).
2. The principles of necessity and relevance governing the collection and storage of personal information.
3. The principle of reducing the collection, use and storage of personal information to the maximum extent possible.
4. The principle of finality (the purpose and ultimate administrative uses for personal information need to be established in advance).
5. The principle of establishing and requiring responsible keepers for personal information systems.
6. The principle of controlling linkages, transfers, and interconnections involving personal information.
7. The principle of requiring informed consent for the collection of personal information.
8. The principle of requiring accuracy and completeness in personal information systems.
9. The principle of data trespass, including civil and criminal penalties for unlawful abuses of personal information.
10. The requirement of special rules for protecting sensitive personal information.
11. The right of access to, and correction of, personal information systems.
12. The right to be forgotten, including the ultimate anonymization or destruction of almost all personal information."