THE NEW PRIVACY ISSUES - AGENDA FOR THE 1990's

Computer matching, compliance audits, genetic fingerprinting, and AIDS privacy policy for employees were all discussed when over 300 access and privacy professionals met in Ottawa in April. The presentations mapped out the privacy issues which will confront companies, data protection authorities and individuals in the 1990's and into the 21st century. David Goldberg reports.

Information Technology and Privacy

Priscilla Regan, Senior Analyst, Communications Information Technology Programme, Office of Technology Assessment, Washington DC, USA noted three technology driven developments affecting privacy:

1. across-the-board computerisation;

2. the use of microcomputers for routine administration (which contributes to the question of what constitutes "a record"); and

3. the evolution from indirect to direct data linkages.

Governmental usage of these developments is leading, in practice, to a national database in conjunction with social security PIN policy, which raises serious questions as to the efficacy of institutional oversight. Privacy concerns tend to be an afterthought, since neither Congress nor the Executive provide a forum for considering new electronic record applications.

However, in June 1989 the Computer Matching Protection and Privacy Act, 1988 (PL&B February '89 p.8) is coming into force. This establishes **data integrity boards** within each federal agency, which would have to:

* approve of computer matches included in online linkages;

* approve and monitor written matching agreements which would veto agency decisions regarding computer matches.

Finally, Regan mentioned the establishment of federal pilot projects:

- one under the auspices of MEDICAID to test an electronic eligibility verifiability programme. This works using food stamp cards or their automated equivalents;

- another under the MEDICAREDRUG system again involving the eligibility of the client.

Regan posed the question as to whether the federal health department had the authority to set up such a system.

Ann Harkins, Chief Counsel, Senate Subcommittee on Technology and the Law, Washington DC, USA foresaw the arrival of a society distinguished by the amount of information stored on each individual with the limits to electronic delivery systems governed only by the criteria of efficiency, cost and national security. Undoubtedly, technology developments drive legal changes, so the question for legislators is always: what laws do we need in the light of what do we need to know? (which itself is determined by technological capability). The Technology and Law Committee, under the chairmanship of Senator Wise, was due to begin hearings on May 15th on the problem of computer viruses. There was some new law in the privacy area. The Video Records Privacy Act, passed by Congress on October 19th last year protects video rental listings (PL&B February '89 p.9). It was brought in after the exposure of the video preferences of Judge Bork, President Reagan's nomination to the US Supreme Court who failed to receive Congressional approval last year.

David Flaherty, Professor of Law and History, University of Western Ontario, and the author of the forthcoming Protecting Privacy in Surveillance Societies, made, perhaps surprisingly, the point that "I do not believe that new information technology as such is the most vital problem facing those interested in data protection in North America." He said that the most vital task facing data protection professionals was to "work hard at implementing existing national, state and provincial legislation." This involves better training, greater awareness of fair information practices and doing compliance audits, in terms of basic principles, the most neglected aspect of data protection everywhere, even within the US Government. However, the Canadian Federal Privacy Commissioner has established an audit team to visit Government agencies and appraise their internal audits where they have been established. For example, the Canadian Security Intelligence Service is audited by a civilian review body, the Security Intelligence Review Committee. Departmental audit reports indicate a "substantial tale of non-compliance with the Privacy Act."

On the private sector, Flaherty mentioned the Video Records Privacy Act, and the data derived from cable TV systems. But he was trenchantly opposed to any continued faith in self-regulation in the private sector. Two other "horror stories" (revealed in the **Privacy Journal**) concern:

* The "super bureau" for reports on individual consumers. The National Credit Information Network Inc. allows its subscribers to phone in and conduct real-time, on-line searches on more than 200 million consumer credit reports, drivers' licence records from 49 states, a nationwide database of Social Security numbers, and certain court records;

* the state of California is ready to issue machine-readable drivers' licences, which will "create the world's largest card-activated digitized database, capable of storing photographs, fingerprints, signatures, ages, heights and weights, addresses and possibly phone numbers for 50 million persons."

Flaherty also spoke about two Canadian issues which are characteristic of those expected to cause concern in the 1990's:

1. The Privacy Commissioner has requested the Canadian Radio-Television Telecommunication Commission not to require Bell Canada to issue its telephone directories in digitized form because it would open the door to uncontrolled matching (PL&B February '89 p.3); and

2. The Dubin Inquiry has uncovered the prospects of an epidemic of uncontrollable and unnecessary drug testing. There is a proposal, for example, to test all inter-collegiate athletes in Canada. The new technology of urinalysis machines heralds a "massive invasion of the privacy of the individual." The Canadian House of Commons Standing Committee on Justice stated in its 1987 Report on the Privacy Act that some high risk employment positions do demand periodic/continuing drug testing, but that "the crucial variable is that such testing has to have some reasonable and meaningful connection to the tasks or employment in question."

Finally, the Canadian judicial position was summed up by Mr Justice la Forest in the case of Queen v. Dyment (December 1988) who distinguished between vindicating the right of an individual's privacy after it had been violated and being secure against unreasonable searches and seizures, which entails clear rules setting out the circumstances in which privacy can be violated. He clearly believes that a proper defence of privacy should extend beyond the first case and include the second.

The New Privacy Issues: What Are They?

Robert Ellis-Smith, Publisher, Privacy Journal, Washington, DC, USA listed a host of areas where developments held implications - not always clear - for privacy defenders:

1. The recent US Supreme Court decision which endorsed the legality of genetic fingerprinting;

2. The introduction of electronic anklets for prisoners;

3. The use by the Food and Drugs Administration and the Securities and Exchange Commission of new technology for complex transactions;

4. There can now no longer be any such thing as an unlisted telephone number; incoming calls' numbers can now be displayed. As a result, services have grown up transmitting batches of "hot line number" inquiries to interested third parties; outgoing call's numbers can, of course be logged. This has implications for employees such as journalists or whistleblowers;

5. Uniform product (bar) codes do not just activate registers and stock inventories. If the information on X's purchases so gathered are passed to e.g. a cablecaster, specific advertisements can be tailored for X's house dependent on that person's purchasing habits;

6. Unsolicited fax-delivered advertisements deprive someone of their telephone line and are a nuisance in terms of filling the office with

unwanted paper;

7. The development of "super bureaux." TRW Inc. was reported in US News & World Report (May 1, 1989 p.52) as selling credit information collected for one purpose for use for another purpose. This resulted in the dissemination of sensitive personal information and raised the question of whether this was a proper use of the information. Did it not lead to the denial of the person's autonomy and their possible manipulation?

8. He criticized Congress' sense of priorities by enacting the Video Records Privacy Act (protecting pornography) rather than a Library Lending Record Protection Act because, of course, that would frustrate the FBI's library checks on who is borrowing what.

9. The United States Supreme Court was criticised for choosing to protect an individual's old criminal justice record (the "rap sheet") but for failing to protect bank records, medical prescriptions or sexual privacy.

10. Finally, the advent of general terrorism and the consequential governmental reaction carries with it the implication that the innocent right to travel is being compromised, and individual privacy, in the sense of autonomy, is being jeopardised.

Ann Cavoukian, Director of Compliance, Office of Ontario Information/Privacy Commissioner, gave what was arguably the scariest presentation, (drawing on the work of Jeremy Rifkin, Director of the Foundation on Economic Trends, Washington DC). She spoke of the implications of the near-future ability to read the human gene code (made up of 46 chromosomes and 100,000 genes). Mapping research, to discover the location and function of each gene, is a worldwide scientific adventure and has led to the creation of the Human Genome Organisation. (Genome means the genetic code providing a genetic human blueprint). Rifkin has written (Algeny: A New Word, A New World) of the 1990's as the Age of Biotechnology, in which the key issue will be the right to genetic privacy. This will be necessary, for the control given by access to genetic information may lead to fresh sorts of discrimination. According to a survey, reported in Time (April 13th 1989), 43% of major multinational companies have already established drug/alcohol monitoring programs for existing staff and job applicants. The future risks are already clear. Several major companies would be willing to introduce genetic screening in the workplace. Such screening would enable hiring/firing decisions to take place on information which is not necessarily based upon a fact, but on an inference from a predisposition suggested by the presence of a particular gene.

A 1988 United States Office of Technology Assessment report said that 50% of those questioned would use genetic screening. This could lead to a demand for a "perfectly healthy workforce." But this neglects the interplay of environmental factors which can affect, or even negate, the outcome of the genetic predisposition. In short, a predisposition in an individual may create a fear of a health problem where none exists.

Cavoukian predicted the creation of central genome databanks, so that rights of privacy will depend on the conditions of creation, accumulation and transfer of the information in them. These would be unlike

any other databanks due to the nature of the information stored therein. Rifkin had called for the setting up of a Human Genome Policy Board. (Since this conference, the UK government has announced plans to establish a DNA databank on criminals, since DNA "fingerprinting" has already helped in criminal convictions).

Eugene Oscapella, an Ottawa-based consultant, made a major contribution to the study published by the Canadian Federal Privacy Commissioner, AIDS and the Privacy Act, published in March this year. He argued that the spread of AIDS is "altering the terms of your membership of society." A number of the sections of this report (PL&B February '89 p.4) deal with issues in the workplace although it is really confined to the implications for the federal government.

1. In general, when AIDS-related information becomes known to an employer or other employees, or those whom the employer serves, "the employee risks dismissal." This may also have implications for the victim if it results in loss of his employee health plan. Is such dismissal acceptable if it is based e.g. on fear following revelation of the employee's life-style? (Part 2, p.9). However, some occupations demand a certain level of mental and physical health; so not only is there pressure to collect and use such information in general, but also it is argued it should be personal, i.e. name-linked information (Part 2, p.13);

2. Should employers develop, or be required to develop AIDS policies? The Canadian federal Health, Education and Welfare (HEW) department has encouraged private sector employees to do this; but so far the Federal Government has not yet completed its own (Part 3, p.15);

3. The Report calls on the Treasury Board to consider the June 1988 "Statement from the Consultation on AIDS and the Workplace" (WHO/ILO); this asserts that pre-employment HIV screening as part of fitness to work assessment is unnecessary and should not be required. If done, for insurance or other purposes, this may lead to unacceptable discrimination. As to current employees, the Statement suggests

    a) HIV screening should not be required, and

    b) confidentially must be maintained about all medical information including HIV information, and

    c) the employee should not be obliged to inform the employer about her/his HIV status, and

    d) employees affected by HIV must be protected from stigmatisation/discrimination in the workplace, and

    e) if fitness to work is HIV-impaired, alternative

working arrangements should be organised; and

f) HIV infection is not a cause for terminating employment; such persons should be able to work on, appropriately, for as long as medically fit.

Thus, the Report Recommends that "Treasury Board take steps to issue a comprehensive policy on AIDS in the workplace; this policy should include a clear statement on confidentiality and the controls on the collection of AIDS-related personal information, guided by the principles and recommendations set forth in this report." (Part 3, p.16).

4. Finally, the Report recommends that if any public service employee is diagnosed HIV seropositive, then only that person's physician or a physician from HEW should know - i.e. not the co-employees or the person's superiors. Such information should not appear on a personnel file, eliminating the chances of a leak, and even if the person volunteers information, it should not be filed.

Responding to a question from the floor, "Will industry want perfect employees for some sectors?" Oscapella replied that "Industry would like to convince us of that." He added that whatever regulations were adopted, they would need to be international in scope because of the internationalisation of business and competition.

It seems as though both the genetic screening issue and the development of AIDS are going to raise delicate issues of privacy which will vex employers in the private and public sectors. Soon, also, there might be questions raised concerning whether certain technically feasible processes will be lawful, partly because of their implications for privacy.

Access 89: Practical Approaches to Access was a conference held in Ottawa on April 13/14th and was organized by the American Society of Access Professionals (ASAP) and the Canadian Access and Privacy Association (CAPA). The meeting saw the inauguration of The Canadian League of Information Professionals (CLIP), mainly a private sector organisation.

For further information on CAPA and CLIP, contact:

Tom Riley, Riley Information Services, PO Box 261, Station F, Toronto, Canada, M4Y 2L5. Telephone: (416) 593-7352.

For further information on ASAP, contact:

American Society of Access Professionals, 2001 S Street, N.W. Suite 630, Washington DC, 20009, USA. Telephone: (202) 462 8888.

David J.A. Goldberg is a lecturer at the Department of Jurisprudence, Glasgow University, Scotland and a consultant on information law.