Some Perspectives on Information Technology and Privacy*

David H. Flaherty
University of Western Ontario
London, Canada N6A 5C2

I am very pleased to have an opportunity to participate in this session and in this important conference. May I begin by congratulating the American Society of Access Professionals and the Canadian Access and Privacy Association on their continuing initiatives in this direction. Workshops such as this one should help considerably in persuading participants that they are engaged in an activity that is vitally important to the public interest in North America.

I want to begin by making a point that may seem a bit surprising, given the title of this session. I do not believe that new information technology as such is the most vital problem facing those of us interested in data protection in North America. Technology has always been with us and will continue to be so. The telephone, the telegraph, the computer-all in their turn posed challenges to the preservation of personal privacy and will continue to do so.

The most vital activity for data protectors like yourselves is to work hard at implementing existing national, state, and provincial legislation. In my judgment, and I have just finished a large comparative book on the subject,[1] improved implementation of existing legislation is the key need. This involves better training of those carrying out data protection activities for governments, heightening public and public service awareness of fair information practices, and, especially, doing audits of compliance with basic principles.

In this connection, Treasury Board Canada deserves congratulations for the schedule of training courses it has arranged for 1989-90 and for attention to the status and role of access to information and privacy coordinators.[2] The work of the Treasury Board and the Privacy Commissioner of Canada illustrate how much better the Canadian system of data protection is than what exists in the United States, a view that I would be pleased to expand on in the discussion period. Even at the state level, there is no American equivalent to the continued accomplishments of the Commission d'accès à l'information in Quebec and the Office of the Information and Privacy Commissioner in Ontario.

But all of these institutional achievements mean little unless the relevant legislation is made to function well over time. In this sense, we are just beginning to make data protection meaningful in Canada (and may I remind you that 8 of the 10 provinces do not even have general data protection laws.)

I am especially interested in promoting internal and external audits of compliance with data protection rules, a process that is only beginning. Auditing and related inspections are the most neglected aspect of data protection in every country; they do not even occur in the United States government.

I am discussing audits in the same sense that is used by John Grace, Barry Baker, and the auditors in the office of the Federal Privacy Commissioner. Guided by a computer-based system of risk

analysis, Baker and his seven auditors are visiting government institutions in order to do detailed inspections of fair information practices. The Privacy Commissioner is also encouraging government departments to do their own internal audits of compliance (a rare occurrence), so that the Commissioner's auditors, a small group of watchdogs, can then audit what the auditors are doing. This model is now working for the Canadian Security Intelligence Service, which is audited first by its own civilian review body, the Security Intelligence Review Committee, which has been chaired with distinction and commitment by Toronto lawyer Ronald Atkey.

My emphasis on the centrality of audits for effective data protection betrays my strong conviction that data protection has much more important tasks than responding to requests from individuals for access to their own information, which, at least in the past, has been the main preoccupation of Canadian federal privacy coordinators. They must broaden their horizons with a more intense focus on sections 4 to 8 of the Privacy Act and thus, in the words of John Grace, truly become "the privacy consciences" of their department.

I have been further persuaded of the centrality of the auditing function by reading some of the Privacy Commissioner's audit reports, which I obtained from government departments themselves. The Commissioner summarized them in his 1987-88 annual report, but I think the actual reports are even more revealing of serious problems found his brief summaries.[3]

As a gesture of thanks to the Access to Information coordinators of the departments who furnished me with copies of the audit reports, I will not name their departments publicly. However, I will mention Transport Canada and Correctional Services Canada, which have yet to respond to my request for their audit reports.

At one government department, the Privacy Commissioner's auditors found: 1) "a general lack of awareness among departmental employees of the Privacy Act, its application and implications;" 2) failure to follow approved retention and disposal schedules for personal information; 3) little or no review of the physical security of the department's personal information, nor any comprehensive review of the department's personal information holdings; and 4) failure to describe personal information banks in the Personal Information Index. Without mincing words, these findings, in my view, amount to a substantial tale of non-compliance with the Privacy Act.

In terms of even more specific findings, the Privacy Commissioner's auditors found that "some files containing personal information are stored in areas ... that are accessible to unauthorized individuals or individuals who have no 'need-to-know.'" Furthermore, "the audit disclosed that individuals throughout the Department maintain duplicate or private file systems that contain personal information, derived largely from personnel records," which increases the possibility of unauthorized disclosure and may result in the denial of individual rights.

The results of the second audit that I have reviewed contain similar negative findings. Added "features" include the storage of personnel files in areas open to the general public and cleaning staff, inadequate physical security, and improper disclosure of

personal information to other federal institutions.

I submit to you that these two audit reports contain devastatingly negative evidence of non-compliance with the Privacy Act. You will forgive me for suspecting that a careful audit of any federal department would probably turn up comparable results.

Let me turn to a second area related to the theme of this session. What should legislators and data protectors do about data protection in the private sector in North America? My premise is that the collection, use, storage, linkage, and disclosure of personal information by the private sector is almost completely unregulated, except for certain credit information laws. As well, in the United States, which has a better track record than Canada in this regard, there are specific federal sectoral laws for cable privacy and video rental lists.

Until the advent of data protection laws for the public sector, privacy advocates like myself have been reluctant to urge general regulation for the private sector and piously proclaimed the virtues of self-regulation. I would submit to you that self-regulation has failed demonstrably in Canada in particular. The Canadian Bankers Association has failed to produce a privacy code. The same holds true for the Royal Bank of Canada, despite similar public discussion before parliamentary hearings in 1986 about their continued progress in this direction. The situation is unacceptable, as we witness the emergence of surveillance societies in which interlinked data bases are monitoring the behavior of each and every one of us. Again, I will be pleased to expand these views in the discussion period.

Those doubting my fears concerning data abuse in the private sector cannot be readers of those two excellent American newsletters, Privacy Journal and Privacy Times, whose editors, Robert Ellis Smith and Even Hendricks, deserve our praise, thanks, and subscriptions for their valiant efforts to awaken privacy consciousness in the public.

The March 1989 issue of Privacy Journal features an article on what are called "Super Bureaus," which are essentially supermarkets for reports on individual consumers. The National Credit Information Network, Inc., for example, allows subscribers to dial its computer directly and conduct on-line, real-time searches of more than 200 million consumer credit reports, drivers license records from 49 states, and a nationwide data base of Social Security numbers, apparently compiled from non-governmental sources. Searchers also have access to date of birth, marital status, and certain court records.

To give only one more brief example, again from Privacy Journal's current issue, California is ready to issue machine-readable drivers' licenses, which will, by 1995, create the world's largest card-activated digitized data base, capable of storing photographs, fingerprints, signatures, ages, heights and weights, addresses and possibly phone numbers for 50 million persons.

I submit to you that these massive data bases illustrate that we already live in surveillance societies. I also believe that governments are going to have to intervene to protect individual rights in the private sector. I applaud the federal government's

initiative in extending coverage of the Privacy Act to crown corporations, am concerned at the apparent efforts of Air Canada and Petro Canada to escape from the rigors of this law, and encourage the federal government to extend the Privacy Act to the federally-regulated private sector, including banks, trust companies, and cable TV companies. I welcome some signs that the Quebec government may be the first to act to ensure data protection from the private sector for residents of that province.

I have one final item to mention briefly. The Privacy Commissioner has opened 1989 with a bang. In January he cautioned the Canadian Radio-television and Telecommunication Commission not to require Bell Canada to provide its telephone directories in computerized form, because it opens the door to uncontrolled matching of subscribers' addresses and phone numbers with personal information from other computerized data bases. In late March, the Privacy Commissioner issued his major study of AIDS and the Privacy Act.

But I am not content to let John Grace and his colleagues rest on their laurels. There is another technological genie struggling to get completely out of the bottle that I think he should be addressing, and that is drug testing. The Dubin Inquiry is liable to unleash unrivalled bottle wars and not just involving carded athletes who compete at the international level. There is a pending proposal to drug test all intercollegiate athletes in Canada, which I regret to say my university is regrettably alone in contesting and questioning. We risk a pandemic of uncontrolled and unnecessary drug testing.

Drug testing is a massive invasion of the physical privacy of the individual, which challenges our constitutional rights to privacy in Canada and the United States. It should only occur when there is at least probable cause of suspicious behavior and evident abuses. It is too easy to believe that urinalysis machines, and comparable technocratic toys, can solve sensitive social problems.

It is worth reminding ourselves that the Supreme Court of Canada is using the Charter of Rights and Freedoms to develop a constitutional right to privacy for Canadians. In Queen v. Dyment, decided last December, the court further developed the sphere in which individuals merit protection from unjustified state intrusions upon their privacy.[4] In his concurring opinion, Mr. Justice La Forest made the following general point: "...if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated."

The House of Commons' Standing Committee on Justice and Solicitor General discussed urinalysis in the context of employment in their 1987 general report on the Privacy Act:

> The Committee acknowledges as a general matter that some high risk positions may require drug testing as a periodic, and even continuing, part of the employment process. The crucial variable is that such testing has to have some reasonable and

meaningful connection to the tasks or employment in question. The Committee considers it unlikely that uniform, blanket testing of all applicants for employment or all employees would be necessary or desirable.[5]

U.S. Supreme Justice Antonin Scalia said in dissent in a 1989 decision on drug testing of U.S. Customs Service employees: "In my view the Customs Service rules are a kind of immolation of privacy and human dignity in symbolic opposition to drug use.... The impairment of individual liberties cannot be the means of making a point; symbolism, even symbolism for so worthy a cause as the abolition of unlawful drugs, cannot validate an otherwise unreasonable search."[6] Need I remind you that Justice Scalia is not a card-carrying member of the American Civil Liberties Union.

My view is that the Privacy Commissioners of Canada, Quebec, and Ontario should join together in addressing the privacy implications of drug-testing before all of us are spending even more time around toilets and urinals than we already do.

Prepared for presentation to the American Society of Access Professionals' international workshop/training session on Access to Information Laws, Ottawa, Canada, April 13-14, 1989.

1 See David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (University of North Carolina Press, Chapel Hill, NC, and London, UK, 1989 forthcoming).
2 See Treasury Board of Canada, Access to Information and Privacy Coordinators: Their Status and Role (Ottawa, 1989).
3 Annual Report, Privacy Commissioner, 1987-88 (Ottawa, 1988), pp. 38-43.
4 See, in particular, Hunter v. Southam, 2 Supreme Court Reports 2 (1984)
5 Open and Shut: Enhancing the Right to Know and the Right to Privacy. Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act (Ottawa, 1987) p. 72.
6 Privacy Times, March 29, 1989, p. 3.