INDIVIDUALS' PRIVACY RIGHTS V. ORGANIZATIONS' PERSONAL DATA NEEDS

The topics chosen for the evening debate at the Cambridge Union, an innovation at July's Privacy Laws & Business 5th Annual Conference, were at the privacy frontier. The extracts selected here are illustrations of the forward looking issues, the sort of privacy issues that we are facing in the coming years, not necessarily covered by conventional data protection legislation.

MEDICAL DATA

Patients are not Packages of Information

Pierrot Peladeau, Ligue des Droit et Libertés, Montreal A director of the Canadian Medical Association once described change in medical practice this way: "A generation ago a physician received at his office a person who would put his or her body in the hands of medicine. Nowadays, physicians receive first a little package of data, they process the data and then treatment of the patient follows. In medical teams, some professionals can even treat patients they will never meet."

While information has grown more important in medicine, other changes have occurred. First, professionals used to keep files in confidence with patients, then the file became part of a clinic or hospital, shared by all professionals working there. Now, the file is being regionalized and shared between different medical institutions and authorities. "What was privileged information between one person and one professional has now become data packages used by a medical system." The information packages are being designed to meet the needs of new interests, administrators, public authorities and researchers.

For example, a new health information system being put into place in Quebec came from administrators, with the object of gathering data on clients in one region from social workers, psychiatrists, counsellors etc., in order to understand "client trajectory" in and out of the medical system and to bring about better decisions. They thought that by sharing files the operation would be more coherent, with services focused on the clients. However, "mental clients do not necessarily want or need coherent intervention;" they choose particular therapists or services for different reasons. The new system is viewed by clients as an infringement on their freedom of choice and their right to suitable treatment. In computerization of medical records over the last 20 years in Quebec, patients are not considered as stakeholders or brought in as part of the design or decision process. They should not be thought of as, "objects of the system...little packages of information, but as stakeholders and human beings. Only then can there be a real discussion on the balance between needs and rights."

Three Employment Cases

Erika Barr, MSc student, London School of Economics presented three of her experiences from actual companies in London and the US. "These are not what-if scenarios, what happens if medical data is lost...these are actual situations that have happened."

Firstly, after eating a spicy meal, a person felt ill and called in sick to work the next morning. At one company, the secretary wrote down the name, put the information on the company's public bulletin board of "people who are sick for today," and fellow employees asked about the illness when the person returned. "Is this a policy matter, is this a privacy issue, is this a security issue? I believe this involves all three."

Secondly, an Information Systems department decided to monitor the telephone calls of its employees and gave the assignment to temporary intern students. After examining the numbers on the database, they decided to call up several numbers called by the vice-president. At one of the numbers a secretary answered "Dr. Smith's office." This is indirect information that was collected without the knowledge of the employees, and

information that was given to people who should not have had access to it. "Clearly bad policy."

Thirdly, after poking his eye, a manager tells his secretary that he's going to the hospital and will not be in for a while. After his return, the personnel office calls him, enquiring, "is your eye OK?" and asks if he needs anything. He is furious! It is none of their business! Does personnel have the right to such information and should the secretary have given it? The argument is that despite the introduction of laws and regulations and the new technology, it is important to understand how personal information flows within organizations and how it needs to be controlled to ensure privacy and security. There should be policies for securing data and to protect the privacy of individuals.

POLICE DATA

Do Not Take Privacy in Isolation

Superintendent Ken Grange, Metropolitan Police - who is the data protection officer for the force, a senior crime investigator and has conducted complaints against officers, said that relatives of victims of serious crimes say "damn your privacy laws, just go find the person who committed this awful crime." The police service has to respect the law, but there are aberrations, especially in issues such as the provision of undisclosed material. "People musn't run away with the cosy idea that data protection legislation will prevent such disclosure. Who knows what hands it is going to get into?" He said the police service is a "low user of information technology." People who think they are loaded with computers holding volumes of information are wrong. The registration for the police national computer permits disclosure to all sorts of organizations, with the blessing of the Registrar's office. For example, the BBC gets information. Especially in "extreme circumstances" such as a bombing outrage, the police might very well like to "get a glimpse" of a video camera at an intersection near the crime, go through parking ticket records to see if the vehicle involved has got a ticket. "Where do you draw the line? It's a balancing act." The Data Protection Act gives special powers to police, especially in matters of national security, demanding disclosure of personal information "provided we can satisfy certain criteria. You musn't take the privacy issue in isolation. It's a big, wide, complex area," but the police do their best to work within the law.

US Police Examine 100,000 Home Phone Records

Professor Joel Reidenberg, Fordham University, New York - A case a year ago in the US raised question of police use of information in Ohio.

A crime was committed by an employee of Proctor and Gamble, who spoke with a reporter at the Wall Street Journal and told him there was going to be a management shake-up at the company. Proctor and Gamble complained to the local police, who got a subpeona of the telephone records to search for which line was used to call the reporter. In the process of the search, the police looked at records of every telephone call made to all citizens in a certain area code, about 100,000 individuals whose home phone records were examined by the police to find the one person.

"It raises the question of what if you are the innocent person who had nothing whatsoever to do with the situation? Here, the police department has now gone and looked through carefully all of your phone records. I think that raises a lot of disturbing questions as to where, if you're collecting information from automatic monitoring of some sort, do you draw the line? What is the legitimate police function to try to track down the criminals? In doing so, how many individuals' rights are you trampling who had nothing whatsoever to do with it, just happened to live in the area code of the state of Ohio?"

Not in the UK

David Hayward, National Executive Committee, the Police Federation of England and Wales - "Just to put the minds of the

audience at rest, we don't have those powers in the UK, we couldn't cope."

TELECOMMUNICATIONS DATA

Balancing Privacy and Consumer Interests

Dr. Adriana Nugter, Privacy Manager, Netherlands Telecom In the area of telecommunications, individuals' rights do not clash with the organization's needs. "Why should we as a telecom operator and service provider not process, collect and use data fairly?" The problem is in other rights, such as consumer rights, in issues such as itemized billing, where her company has had discussions with interest groups, privacy groups, health organizations and found that customers have a right to know what they are billed for, but also a right to have their privacy protected, both as the person making the phone call and the person seeing his phone number displayed on another person's bill. To balance these two interests of privacy and the consumer, the company came up with the solution that every subscriber has the right not to have his number displayed on another person's bill, a satisfactory solution to counterbalance both interests.

Police and tax authorities have a growing interest in telecommunications data, such as mobile subscribers. "Police have great interest in having location data. Should we give them this data, should we give them only in specified cases or should be just have them generally available for them on every request for help? Tax authorities also are very interested to have access to all of the telephone call records. They would like to check out whether you have made these calls for a business purpose or for a private purpose. Should we keep this data for 10 years, like most tax laws require?" She said it is important to discuss these issues, rather than discuss whose needs take precedence in the motion.

Human Dignity Strangled by a Telephone Cord

Prof. George Trubow, Center for Informatics Law, John Marshall Law School, Chicago - said "let's choose sides and call for personal freedom." He said telephone companies in the US are "far more a frightening thing" than that described by Ms Nugter in The Netherlands, adding that there is a conflict between telephone companies and data subjects. Caller ID, where the telephone number of a calling party is displayed on the telephone of the person who receives the call, is presented by the phone company as a matter of protecting the privacy of the person called. He said there should be a blocking device available to the caller, to protect his privacy, "and the person who's receiving the call doesn't have to answer the damn phone if he doesn't want to." The phone company wants to charge for the right to block. "My position was that's like giving somebody a disease and then selling him the cure...If you're going to put this caller ID in, you're going to give me the blocking mechanism without charging me for it."

In Illinois, Caller ID with a free blocking mechanism has been implemented. "Let us be sure that we do not let personal freedom and human dignity be short-circuited and strangled by a telephone cord...It is the right of the individual, the data subject that is concerned here." He said one attitude is that "a little privacy is OK but not too much."

Free Call Blocking in Canada

Stephanie Perrin, senior policy analyst, Canada's Federal Dept. of Communications, Ottawa - after the "dog's breakfast" of judicial debate in the US over caller ID, there has been a decision in Canada permitting free call blocking. "The fact is that the call managment services are selling very nicely, they are making quite a bit of profit," and the economic argument against offering blocking is not legitimate. On data subjects' views, the department of communications in Canada is having a full public debate on privacy interests in telecommunications. If other public services did this there wouldn't be messes such as that surrounding Caller ID. "The obvious problem with understanding of these technologically privacy-invasive services is nobody knows

anything about them; the level of ignorance is appalling. The only way we can correct that is through full public debate."

Individual Needs to Maintain Control

George Trubow - When the Illinois Public Utility Commission required the telephone company to give it some rate projections regarding caller ID operations, they said they would make $90-million a year with Caller ID, only $60-million with the "block" feature. On the issue of ignorance, "Ma Bell" never told the public what was at the bottom of the caller ID controversy. "I believe caller ID is a red herring, a stalking horse...I believe that it is an attempt to get unbridled authority to send forward information about a telephone user without his knowledge or consent. This is essentially what caller ID, without block, opens the door to, the ability of the phone company to send information about you forward without your knowledge or consent simply because you are a telephone user. The information available to the phone company is incredible. As our phone company likes to say, "we're all connected," and it's those connections and the data flow that create the problems. The individual needs to maintain control over information about himself."

Free Blocking Pre-Condition for CLI in UK

Dr. John Woulds, Senior Assistant Registrar, Office of the UK's Data Protection Registrar - said Oftel is not the only regulator. The Data Protection Registrar recently commented that CLI is within his jurisdiction and he feels that provision of CLI without free, simple blocking for the caller will be an infringement of the Data Protection Act.

This report is by Mary Gooderham, a writer on privacy and technology.

Her full debate report is available, with the PL&B Conference papers, from the PL&B office.

PRIVACY INTERNATIONAL ADVOCATES STRONGER RIGHTS

Privacy International, with members in neary 50 countries, is an independent, non-profit and non-partisan organisation that seeks to "raise awareness of violations of privacy rights and to establish limits to the unreasonable surveillance of individuals." It supports the Universal Declaration of Human Rights and the privacy principles of the Council of Europe and the OECD.

At its inaugural meeting in Washington in March, resolutions were passed which supported the strengthening of privacy provisions in the European Community, Australia, Canada, Spain, the USA, on "privacy violations against the poor" and on the transfer of surveillance technology to developing countries.

Privacy International's chairman is Jan Holvast, veteran privacy campaigner in the Netherlands and director of Stichting Waakzaamheid Persoonsregistratie (Privacy Alert). One of the Deputy Chairmen is Professor David Flaherty of the University of Western Ontario, author of *Protecting Privacy in Surveillance Societies* (PL&B December 1989 p.29).

An information meeting was addressed by Professor George Trubow of the John Marshall Law School, Chicago and Pierrot Peladeau of Canada's Rights and Liberties Foundation, at July's Privacy Laws & Business 5th Annual Conference in Cambridge. Both speakers also participated in the privacy debate (see above).

Privacy International can be contacted through Marc Rotenberg, Secretary General, Computer Professionals for Social Responsibility, 666 Pennsylvania Avenue, Suite 303, Washington DC 20003, USA, Telephone (1) 202 544 9240 fax (1) 202 547 5482, or Simon Davies, Director General, Privacy International Directorate, Faculty of Law, University of New South Wales, PO Box 1, Kensington NSW 2033 Australia.