CAN THE DATA MATCHING EPIDEMIC BE CONTROLLED?

The threats to privacy from public sector data matching have received relatively little attention, although this data is often more sensitive than that held in private sector files. Meanwhile, in some of those countries where the adequacy or equivalence of the legislation is in doubt from the perspective of the EC draft directive, some first steps have been taken to address the problem.

In the USA, the Computer Matching and Privacy Protection Act became law in late 1988. Canada has Data Matching Guidelines. On January 23rd this year, Australia's Data-matching Program (Assistance and Tax) Act was enacted. It provides legal authority for a matching programme to be carried out under the scrutiny of the Privacy Commissioner. Australia's experience may help place public sector data matching higher on the European privacy agenda. Graham Greenleaf, Chairman of the Australian Privacy Foundation, explains the new legislation.

Data matching is the comparison by computer of two or more sets of personal information which have been collected for separate administrative purposes, in order to identify anything which may warrant further investigation. For example, people who state their incomes differently to different agencies where this is not normally allowed are likely targets of matching schemes.

Former Canadian Privacy Commissioner John Grace described one of the dangers of matching as the conversion of a presumption of innocence into a presumption of guilt. "Thus do old-fashioned fishing expeditions pose as high technology." The Australian Privacy Commissioner Kevin O'Connor calls it "the privacy equivalent of drift-net fishing".

Despite these dangers, the attractions of data matching to adminstrators as a device for reducing fraud and overpayments are very strong. Some of the existing matching schemes in Australia exist only on the most tenuous legal bases, since many of the programmes may have originated in response to administrative demands or as cost saving measures rather than usage authorised by law.

Significant Expansion of the TFN

The new system of reporting taxable income required by the Taxation Laws Amendment Act 1988 involved an upgraded Tax File Number (TFN). Privacy advocates and the Opposition parties had only accepted the TFN system as a reasonable compromise between the protection of privacy and government revenue collection, on the basis of assurances by the government that this would be limited to tax administration, and because of the creation of a Privacy Commissioner who would act as a privacy watchdog.

In the August 1990 budget, the Government proposed that TFN numbers could also be used in a data matching scheme which would match information concerning Commonwealth "income supports" benefits together with taxation information and, for some purposes, Electoral Roll and Medicare identity information. This was a very significant proposed expansion of the use of TFN.

The Senate Standing Committee on Legal and Constitutional Affairs had warned that the TFN system should only proceed if it was "strictly limited" to taxation purposes (Report on Feasibility of a National ID scheme; Tax File Numbers, October 1988). One of the privacy concerns about the extension of the use of the TFN number was that, once it was no longer limited to tax administration, there was no logical boundary to its further expanded use. The question now being asked is, could this extended TFN system be the Australia Card (national identity card) system being introduced by the back door?

The Data Matching Program (Assistance and Tax) Act 1990

Despite these concerns, eventually, the Coalition parties supported the Government to

enact this significant and controversial piece of legislation, and the Data Matching Program (Assistance and Tax) Act 1990 entered the statute book. The Act has a complex structure which is nevertheless becoming standard for Australian Privacy law. The Act states the key principles with which the agencies must comply; it then empowers the Commissioner to supplement those principles with guidelines which are mandatory, and it includes as a Schedule an interim set of Guidelines governing the establishment of the scheme as a whole.

Resulting limitations for the Commissioner

The result is that the key principles stated in the Act implicitly impose limitations on the content of the Commissioner's Guidelines, as they are subordinate to the Act. Both the principles and the interim guidelines also serve to give the Commissioner a positive guide as to what to include in his final guidelines.

The Act provides legal authority for a matching program, aspects of which would otherwise be illegal under the tax file number legislation and the Privacy Act (see PL&B April 1990 p.13). Designated officers of the Department of Social Security now constitute the Matching Agency, and are responsible for carrying out the matching program authorised by the Act on behalf of the other assistance agencies, the Taxation Office, and itself.

A data matching "cycle" must be carried out in accordance with a sixteen stage process (grouped into six steps) which govern the movement of information between the four "assistance agencies" responsible for the benefits mentioned and the Taxation Office. Confirmatory identity information from the Electoral Office and Health Insurance Commission is also used. The Tax File Number is used in some steps of the process, but not others.

There are three main purposes of the matching programmes:

1 to detect people who are obtaining benefits from from two different assistance agencies (eg. pension and student benefits) because they have not informed each agency of the other benefit ("payment matching");

2 to detect persons who have incorrectly stated their income to an assistance agency, by comparing their income details as known to another assistance agency or to the Taxation Office ("income matching"); and

3 to detect persons who have incorrectly stated their income or eligibility for rebates or deductions to the Taxation Office, by comparing what is known about their finances to assistance agencies.

The matching is therefore three way: between assistance agencies; from tax to assistance agencies; and from assistance to tax agencies. All matching takes place via DSS in its new role as the "matching agency."

Balancing accountability and privacy

The Act empowers assistance and tax agencies to take action against the person they suspect might be fraudulently claiming benefits or evading tax, such as cancelling benefits or issuing tax assessments. The claimant has 21 days notice to show why such action should not be taken.

It therefore becomes crucial that the quality of information forming the basis for such an action is beyond doubt, otherwise large numbers of people would be forced to justify their honesty. The interim guidelines do nothing to dispel the anxiety this creates, and in his final Guidelines the Commissioner must address this matter of the integrity of information. The agencies are required to provide periodic cost/benefit and other analyses of the programmes to the Commissioner, (who must report on compliance with the Act and Guidelines in his Annual Report), and a technical standards report must also be prepared dealing with data integrity and security features, but this is not required to be made public. The agencies are also required to report their data matching activities in the Commissioner's Personal Information Digest,

and to advise people whose data is likely to be used of this likelihood.

Data Matching Draft Guidelines lack teeth

In October 1990 the Privacy Commissioner issued draft Guidelines for all types of matching by Commonwealth agencies. The Data Matching Programme Act was based substantially on them. However, these Guidelines are not mandatory. The most they can do is to indicate the Commissioner's view of what conduct is likely to breach an Information Privacy Principle.

If the Commissioner or a complainant seeks to take action against an agency because of a breach of the Guidelines, enforcement will be a problem. The draft guidelines do require agencies to expose their proposals for data matching to public comment, but there is no provision to deal with objections to proposals. Data matching is such a significant form of invasion of privacy, (and there are dozens of agencies involved in existing matching practices), that there should be no confusion of authority and enforceability.

Data surveillance - other developments

The "big picture" is one of an increasingly interlocking network of Commonwealth surveillance systems, under very varying degrees of control. Some examples:

- The Health Insurance Commission is now responsible for the Pharmaceutical Benefits Scheme, so that Medicare, whose card and numbering system is involved, has now become a multi-purpose numbering system. Unlike TFN, this is not subject to detailed privacy controls.
- The Law Enforcement Access Network (LEAN) involves the Attorney General's Department constructing a massive database of "publicly available information." It is being established, without any specific legislative authority or control. The privacy implications of access to and use of public record information need be addressed by the Privacy Commissioner and Parliament as a matter of urgency.

This is an edited version of an article by Graham Greenleaf, Senior Lecturer in Law, University of New South Wales, Australia, and Chairman of the Australian Privacy Foundation, published in the *Australian Law Journal*, April 1991.

NEW ZEALAND'S NEW PRIVACY BILL

On August 10th 1991, Justice Minister, Douglas Graham tabled The Privacy of Information Bill in the House of Representatives. He referred to New Zealand's need to be aware of the demands made by the European Community's data protection draft directive. The bill was passed to the Justice and Law Reform Committee for detailed study. The bill was tabled as part of the budget package in an attempt to combat welfare fraud by conducting data matching.

The first stage is due to enter into force by November 1st this year, the date when the data matching programme is due to begin. The bill provides for data matching programmes to be approved by a Privacy Commissioner in accordance with set criteria.

The second stage is expected to enter into force in the first quarter of 1992. This will grant a right of access to information held by Data Holders or Controllers in both the public and private sectors. Complaints about gaining access to personal data may be made to the newly established Privacy Commissioner. Jurisdiction is given to the Human Rights Tribunal to grant exemptions from the bill's privacy principles in both the public and private sectors. When the second stage comes into force, the Wanganui Computer Centre Act 1976 will be repealed and its Privacy Commissioner's work will be taken by the new Commissioner.

The Justice and Law Reform Committee will now study this proposal together with a privacy bill submitted earlier this year by Opposition Member of Parliament, Peter Dunne.