nature

January 1 & 8, 1976

# Snooping with a CRT

A nurse with access to health records by means of a computer terminal types in her boy-friend's name and finds his medical history. It is not all she would have hoped for. She breaks it off with him.

A defendant in a well publicised civil case has an alibi which the court accepts. A credit card company employee, out of curiosity, calls up his file and finds that his alibi is not borne out by the list of his transactions.

A hotel booking clerk uses a computer terminal to check on a putative guest and finds that a year ago, in a different hotel, he left without paying for his room. The guest, immediately on discovering his oversight, had paid the bill by post. But this correction never got into the computer. He is told the hotel is full.

---

THESE are three of the diverse ways in which computers can facilitate information-collecting in somewhat murky circumstances. The Home Office has recently published a White Paper on Computers and Privacy (Cmnd 6353, 28p), and with it a summary of an interdepartmental working party's review of computer usage in the public sector, with particular reference to safeguards to protect privacy and confidentiality. Back in 1972 Sir Kenneth Younger's Committee on Privacy reported that, although there was no evidence that the private sector was using computers to threaten privacy, there was need for vigilance, in the form of an independent body to review the gathering and processing of personal information. The Younger Committee also gave the government gratuitous advice that such an independent body could, in addition, study the public sector. This White Paper advances the cause of a Data Protection Authority to oversee the handling of personal information. It also gives some reassurance that, in as far as the evidence exists, the use of computers to impinge on people's private lives is not on the increase.

Privacy is a misnomer. We are really talking of the use of personal information for purposes other than that for which it was supplied or collected, and the use of inaccurate or incomplete data where the person reported on has no chance to challenge the accuracy or completeness.

Computers is also a misnomer, so to say. Computers have not, up to the present, created new opportunities for misuse of information; they have simply made possible quicker and larger operations, allowing instant decisions to be made. Newspapers, or gossip in the staff canteen, still have the potential for much more damaging intrusions into the life of the individual than do computers. Nonetheless the computer, with its 1984 image, attracts a lot of the fire, and is often credited with monitoring skills that it does not possess.

The average reader of *Nature* would, however, probably settle for more automation in dealing with public and private enterprise. The tedium of paying separate bills for mortgage, licences, utilities, insurance —of having different numbers for health services, tax authorities, passport, bank, telephone, credit cards— often niggles; roll on rationalisation. But one third of the population of the UK regards it as an invasion of privacy even to have publicly available lists of names and addresses such as electoral lists or telephone directories. With such extremes of opinion, is there any hope that a statutory agency such as the White Paper envisages can satisfy everyone that information is not being misused?

The Younger Committee put forward ten principles for the handling of personal information in computers, including one that "there should be arrangements whereby the subject could be told about the information held concerning him". The White Paper proposes more —"the subject should also be able to find out what has been done with the information, and to whom it has been given". In a society of technocrats, we would all receive a weekly listing of what was held in data banks about us, and by whom that information had been used; the big advantage of storing information in computers, of course, is that all usage can be logged. If we found someone had been nosing around without authority, we would call our lawyer. But that one third of the nation which does not even want names and addresses listed probably has little idea of what to do if supplied with computer print-outs. It certainly is not in the habit of consulting lawyers.

Here, then, is a real job for the Data Protection Authority—to make sure not only that everyone knows what the information they have provided is being used for, but also that ways are devised for fighting misuse at the level of the individual. Many of the biggest threats to the individual, after all, do not come from the computer at all. But perhaps an imaginatively appointed Data Protection Authority, not stuffed with "the good and the great", might lead the way towards broader initiatives to look after those in greatest danger of being trampled on.