Cops call the shots

Police intelligence systems are gathering information on who we are, who we phone and where we go – and they don't even need a warrant.

Duncan Campbell

***Guardian*, 27 September 1997**

ANYONE READING this may already have had details of who they telephone or are phoned by fed into police computer files, it emerged last week after details of automatic links between BT and police computers were described in public for the first time. Delegates to an international conference on economic crime in Cambridge were told that the number of requests for BT data from the police and other agencies was doubling every year, and could involve thousands of people in the course of just one investigation.

Not just phone calls are now logged into police computers, it was revealed. All vehicles entering or leaving the City of London or British seaports are being watched by robot automatic number plate scanners (ANPS), which feed the data to the Police National Computer (PNC) in Hendon. The PNC replies within five seconds if the vehicles are "of interest" to police.

Daryl Godivala, head of BT's Network Special Investigations Department, explained to the conference that BT has met ever-increasing police demands for details of customers' calls by installing an automated computer-to-computer "interface" to feed call information out. Unlike telephone tapping, warrants are not required before confidential data is sent out by BT.

All British telecommunications operators, including mobile phone airtime suppliers, are storing and handing over this information, although only BT runs an automated system. BT says this has been done to minimise cost in the face of escalating and

hitherto uncoordinated police requests. Other UK telecommunications companies and mobile phone operators normally supply data only on paper.

Currently, BT receives and processes about 1,000 requests a week, Godivala indicated. Most requests were for details of subscribers' names and addresses, he said, rather than the numbers they had called.

But the traffic in personal call information is already so large that two British firms have produced special software to automatically process BT telephone call data for intelligence purposes. These systems — called iTel and CaseCall — are currently used by every British police force, as well as by Customs, MI5 and the National Criminal Intelligence Service.

Once received, the data is sifted and transformed into pictorial networks and charts of who talks to whom. To these are added bank records, housing information, vehicle details, and information from inquiries, newspapers, the Net and informants. The resulting charts are often so comprehensive and complex as to back up the most robust of paranoid nightmares. But is it only the guilty who have cause to be worried about the new intelligence systems?

According to intelligence analysts who have designed and used telephone call analysis systems, a single investigation — particularly drugs cases — can eventually result in requests for information about calls made by hundreds or even thousands of telephone customers. Names and addresses of customers called by a suspect are traced and fresh requests sent in to get their calls. The result is an ever-widening circle of people who have been called by people who have been called (and so on) by the original suspect.

One Cambridge detective present claimed that this method had worked well for his force after he had downloaded information on “thousands of calls” and used it to help break a computer theft ring. Cambridgeshire police crime analyst Cliff Nicklin said £500,000 of stolen equipment had been recovered.

In theory, all requests for BT information such as the name and address of a particular subscriber, or the numbers they have called over the previous three years, have to be approved by a senior police officer, of the rank of assistant chief constable or above. In practice, the senior officer’s approval is delegated to more junior officers operating the link computer, and is forwarded automatically from their computers to BT — whose computer centre authenticates the request, and then downloads the information required.

Foreign police and security specialists expressed surprise at the scale and growth of the British telephone surveillance system. In the US, Canada and most European states, a judicial warrant (at least) is necessary to have access to telephone call records. An official from the Canadian Security Intelligence Service said he was “astonished” that such privacy-sensitive information was so freely handed over. A French investigating magistrate said that in France the police would not be permitted to have such information without judicial approval.

Inevitably, many of those whose telephone numbers are caught in the ever-enlarging web of a criminal investigation will be innocent of any involvement other than sharing the same dentist, doctor, school or uninvolved acquaintances. They could even have been a victim of the suspect — or just a wrong number.

Unlike the guilty, however, the innocent have no right to know that their personal telephone call information has been downloaded by BT into police, customs or security service computers. The Data Protection Act requires both the police and BT to keep full records of disclosures. But the subject whose privacy has been breached

is not entitled to find out that disclosure has taken place, even long after an investigation has been concluded.

The BT-police “interface” was one of a range of novel police resources explained to delegates concerned with fighting international fraud and economic crimes, especially on the Net. They were also told about the latest developments at Britain’s PNC which, according to PNC director John Ladley, are leading to “much better support for intelligence-led policing”. Many new systems had been introduced in the mid-1990s, and more were scheduled.

Among these were Quest, which can search the 5.5 million names in the Criminal Names index by reference to factors including accent, associates, “habits”, places and addresses, and even shoe sizes. The recently enlarged names index also includes information about DNA samples and photographs, and is linked to a 4.25 million name fingerprint index. Quest is expected to be fully operational early in 1998.

For vehicles, the PNC is offering Vods — a vehicle owners’ descriptive search — which can answer questions such as: who owns a blue Volvo and lives in this postcode district? Searches like that have previously been too time-consuming to be used in most cases. Ladley also expects the use of automatic number plate scanners to rise dramatically as more and more police chiefs decide they want them.

Currently, scanners send in up to 80,000 checks a day. The PNC anticipates that this use will soon quadruple. All such inquiries are stored for data protection and auditing purposes. This means that historical records from the ANPS system could also be “mined”, for example to analyse patterns of foreign travel.

The little-noticed and still progressing revolution in police information technology has resulted in the employment of growing numbers of police intelligence analysts who use powerful computer systems to visualise and analyse the meaning of the massive and growing data inputs from cameras, telephones and bank records as well as traditional police sources. Neither these jobs nor the computers to back them up existed in the 1980s.

Britain's market leaders in intelligence systems are two Cambridge-based IT companies, who showed off their latest wares last week.

One of them, i2, claims its Analyst's Notebook is used by all British police forces. The Notebook was used to produce charts for such high profile cases as the Frederick and Rosemary West murder case and for City fraud investigations. i2's Web site (http://www.i2ltd.demon.co.uk) offers an animated demonstration of how investigative charts are assembled from myriad data inputs. The company describes its "network analysis" sub-system as particularly useful for "Internet traffic", as well as for "telephone transactions" and [bank] "account transfers".

The Harlequin group (http://www.harlequin.com) says that its system, Watson, is used around the world to investigate fraud, drug trafficking and organised crime. It too produces large and elaborate charts. Watson is designed to draw information directly from the standard Home Office large major inquiry system — Holmes for short. Watson uses artificial intelligence techniques to automatically distinguish relationships between people, places and objects from the data that is fed in.

For the potentially guilty but not the innocent, recent legal changes mean that defendants can level the playing field by asking the police to hand over their databases.

The 1996 Criminal Procedures and Investigations Act requires the police to record inquiries from beginning to end, and to reveal all their material — used or unused — to the Crown Prosecution Service. If information given to the CPS suggests that the the defendant might be innocent, or casts doubt on the reliabilty of prosecution witnesses, the defence has to be told.

Judges have already made at least two orders for the police to copy Holmes databases for the defence to analyse. On the first occasion, however, defence lawyers had no idea how to read the data they were sent. In the second case, which is still sub judice, specialists have been retained to advise on how to interpret and analyse the police data.

Both sides of the courtroom are thus having to come to terms with the new era of electronic transparency. But, as the law stands, the innocent and uninvolved still have no right to know — let alone protest — that their data too has been mined and “warehoused” for future use.