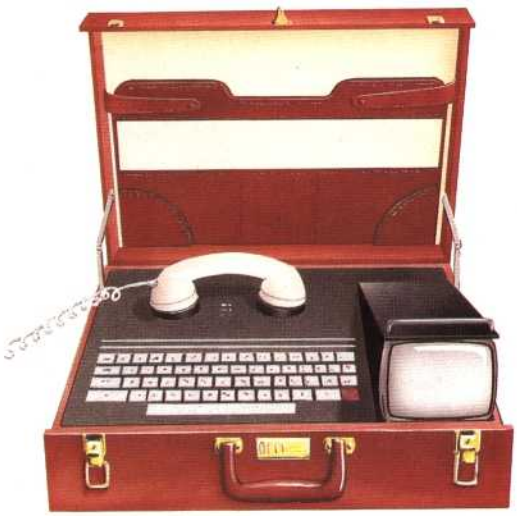
Tools Of The Trade

Computerised Protection
Many executives, and people who deal with classified information, are protecting themselves from electronic spying with gadgets like this computerised telephone scrambler. Instead of speaking on the telephone, the user types his messages on the keyboard. The scrambler sends the message in a 'silent' form over ordinary telephone lines. The message is then received on a matching system's built-in screen. A built-in voice synthesiser can also convert the incoming message into audible speech at the touch of a button



Coded Message
Similar to the computerised scrambler, this system sends a scrambled message from a handwritten note. The scrambled message is protected from eavesdropping and bugging because it is sent silently. Even signatures can be sent in this way

Stress Analyser
The voice stress analyser measures the amount of stress in the voice and displays its results instantly in a simple numeric readout. This is really a sophisticated lie detector and can also indicate whether the person is anxious or tense

stored prints per day.

A similar pattern recognition and comparison system is mounted on a bridge across the M1 motorway, with cameras pointing down at each lane. This system actually captures pictures of the number plates of approaching cars, then uses computer power to analyse the pictures and check the numbers against a file of wanted cars. The information that one of the wanted vehicles has been seen can then be radioed direct to motorway patrol vehicles who will intercept the car.

Initially, the police did not publicise this achievement very much, and the first real public notice was taken after a journalist on the *New Scientist*, Steve Connor, noticed the cameras and asked what they were for.

One obvious area in which developments in microcomputer hardware have had a major effect is the production of smaller and smaller surveillance devices — that is, bugs. Chip technology has made it possible to produce radio transmitters the size of a grain of rice, with sophisticated control electronics built in. A typical device 'bleeds' its power from the Post Office's electricity supply to the bugged telephone, and only switches itself on when someone is actually speaking. Then there are self-powered bugs, equally tiny, that are dropped in the corner of a room and pick up all conversation in that room — once again only working when someone speaks — for transmission to a distant receiver.

Even more in the style of James Bond, there is a 'distant' bug that fires a laser beam at a window. The vibrations of the glass caused by conversation are picked up as interference in the reflected laser beam, and the speech information is retrieved from this interference — by computer, of course.

In military operations, as opposed to undercover security work, the computer operators have the opposite problem. They aim to avoid being monitored by others, and once again chips and computers have come to the rescue. Today's battlefield radio transmitters and receivers use frequency hopping — processor-controlled jumping from frequency to frequency according to a preset code — to avoid eavesdropping and jamming.

Computers in surveillance and security are, at the moment, big machines of the type and power used for complex code-cracking at places like the CIA and the National Security Agency in the US — not to mention Britain's MI5 and MI6. But the advances in hardware technology mean that fingerprint recognition — perhaps even face recognition — will soon be automated and made very inexpensive.

In the future, it is possible that police cars will be equipped with onboard computers that could instantly pull out data from a school record, criminal record, medical record, social security record or any other official file. All this would be accessed by sliding a plastic national insurance card into a slot in the computer. The machine would accept fingerprints and a photograph, compare them with central files, and make sure of the suspect's identity.

This might seem a paranoid vision, but the technology is there, or almost there, to do this now, and there are people in the law and order lobby who would like to see it done.