



MIND THE BUGS DON'T BITE

PAUL HAWKES

Directors often express surprise at how prolific transmitting devices (bugs) are in the marketplace. The concept of being bugged is indigestible to many, but the facts speak for themselves. Hundreds of thousands of covert listening devices are bought in the UK each year, all supposedly for legal purposes, which means for both private and corporate concerns. The simple rule of thumb is that it is legal to listen, if you own the phone.

There are times when covert telephonic recording needs to be employed to assist in uncovering damaging corporate disloyalty or fraud, and when companies need to protect themselves from those employing illegal and potentially damaging eavesdropping techniques. Many responsible for contracting counter-surveillance to detect the presence of transmitting devices talk about the service being a peace-of-mind exercise.

But let me relate something told to me by a bugging expert working for government services in Northern Ireland. Most counter-surveillance equipment locates transmitting listening devices in operation on or near to the site being swept. High-quality transmitters hide at frequencies just below local radio stations and are typically sold to clients as being able to identify bugs transmitting at these hidden frequencies and as being the same equipment used by government.

True, but it misses some important points. Experienced bugging professionals are able to bypass this system by entering the telephone system between the handset and the exchange, typically at the distribution point, commonly referred to as the green box, which stands on many street corners.

Each phone line has a route from its original location to the exchange. When the green box is near to the phone lines being

tested for transmitters, a transmitter hidden within or nearby may be picked up by the ultra-sensitive electronic equipment.

However, detection can routinely be avoided: Each line takes up two terminals in the green box, and sometimes the box is far enough from the phone to avoid detection. If not, invisible wire (almost unnoticeable) connects the two terminals to 'spare' ones, creating a spur.

The spur is then led to the back of the

'THOUSANDS OF COVERT LISTENING DEVICES ARE BOUGHT IN THE UK EACH YEAR'

green box and the wires are fed out of the back where a transmitter is put in place. The transmitter may then be remotely monitored by a receiver/recorder secreted nearby, typically in an empty, unregistered vehicle. The vehicle can then be visited, day or night, to retrieve tapes of conversations.

Four years ago, I was asked to look into a small energy company in Chelsea. They were aware that information was leaking to a known competitor and it quickly became clear that this was via tapped-into phone conversations. I first conducted a sweep for illegal transmitters and recording devices using government-approved equipment. No illegal transmitters were identified. However, a search of the local green box situated a quarter of a mile away on the Thames embankment revealed a crystal controlled transmitter.

As the receiver was probably hidden in a

nearby vehicle, the equipment was removed and a discreet tamper-evident seal placed on the green box to assist future observation. My client thought surveillance of the green box was not cost-effective and was relieved by the retrieval of the eavesdropping device. A system of regular checks on the tamper-evident seal initially showed that the box remained unopened. But four weeks later, it was. A search found the original set-up was not reproduced, but wiring was fiendishly put in place diverting a spur to spare terminals, which in turn were diverted.

We eventually found the transmitting device hidden behind a green box in Pimlico. A nearby car was later identified as being the container for a receiver. The culprits were never identified, as our clients were not interested in pursuing or funding such an operation. However, they did invest in preventative measures, including ongoing sweeps using technology to scramble communications.

With the advent of digital technology and encryption, this is now much easier. Unfortunately, so is bugging. As part of my ongoing education, I now regularly entertain those I know to be involved with active bugging and continue to have my eyes opened to their ingenuity. So, when you next contract a sweep, ensure it goes beyond a peace-of-mind exercise. And remember: the bugging specialist is a professional in avoiding detection. Know the enemy and stay one step ahead. **ISM**

PAUL HAWKES is the senior partner of Research Associates and has practised as a professional investigator and competitive intelligence consultant for over 25 years.
paulhawkes@investigationservices.co.uk