



ISSUE # 9 - AUGUST 2010

CORPSEC TSCM NEWSLETTER

IN THIS ISSUE

- CELL PHONE SPYING
- MORE EYE SPY THEN I-PHONE
- NEW TECHNOLOGY MEANS THAT BUGGING IS EASY



CELL PHONE SPYING

Dozens of programs are available that'll turn any cell phone into a high-tech, long-range listening device. And the scariest part...They run virtually undetectable to the average eye.

The service promises to let you "catch cheating wives or cheating husbands" and even "bug meeting rooms." Its tools use a phone's microphone to let you hear essentially any conversations within earshot. Once the program is installed, all you have to do is dial a number to tap into the

phone's microphone and hear everything going on. The phone won't even ring, and its owner will have no idea you are virtually there at his side.

MORE EYE SPY THAN I-PHONE AS SMART DEVICE DOES THE LEGWORK FOR POLICE

Criminals using the Apple iPhone may be unwittingly providing police with a wealth of information that could be used against them, research has revealed.

As the device grows in popularity, technology experts and US law enforcement agencies are devoting increasing efforts to understanding its potential for forensic investigators. While police have tracked criminals by locating their position via conventional mobile phone towers, iPhones offer far more information. "There are a lot of security issues in the design of the iPhone that lend themselves to retaining more personal information than any other device,"

NEW TECHNOLOGY MEANS THAT BUGGING IS AS EASY AS A WALK IN THE PARK

It remains a golden rule for spies of any persuasion that a walk in the park is still the safest environment for receiving secret information verbally from an agent.

Anything divulged inside a building or a private car is potentially open to an extraordinary array of electronic bugging devices or telephone intercept systems. Bugging is a fine art, and the technology has leapt forward in recent years.



The electronic bug allegedly used by the police to eavesdrop on the conversation between Babar Ahmad, suspected of having links to terrorist organisations, and Sadiq Khan, his constituency MP, during a meeting in Woodhill prison in Milton Keynes, was probably the conventional type.

The basic form of bug requires someone to listen in from several hundred yards away, or to have a recording system hidden nearby that can store many hours of conversation.

However, the latest electronic listening device is known as the GSM bug. Michael Marks of Spymaster, a company that supplies surveillance equipment, told *The Times*: "With one of these new bugs, all you have to do is place it covertly under someone's desk. It's like a miniature cellular phone. You can ring it from thousands of miles away, it answers silently and you can listen in on conversations. The GSM bug could be in an office in London but the person listening to the conversations could be in Australia."

Prison cells are not bugged routinely, but in the past there have been examples where conversations between terrorist suspects and other prisoners have been overhead by means of hidden listening devices.

In the recent trial of four Pakistani-born terrorists who pleaded guilty to plotting to kidnap and behead a British Muslim soldier, it was revealed that MI5 had entered the house of Parviz Khan, the ringleader, and planted bugs. That break-in would have required a warrant from the Home Secretary.

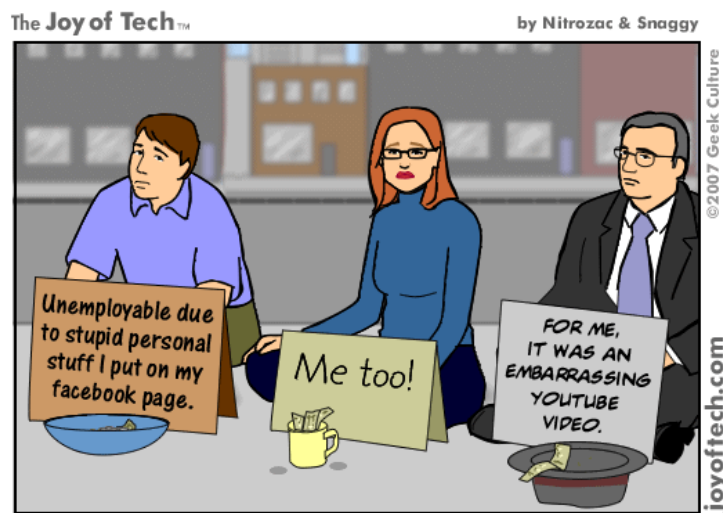
Although electronic bugs remain the staple diet of the surveillance community, the mobile phone has provided a revolution in eavesdropping techniques. They can be used as bugging devices themselves, simply by placing them covertly in an office or home being targeted and switching them on. Mobiles that double as listening devices can be bought on the internet.

Terrorists are fully aware that encrypted mobile phones are vulnerable to eavesdropping by the authorities. "If you can acquire the service number of the mobile phone, what's called the IMEI number, located just under the battery, you can tap in to people's conversations," Mr Marks said.

Terrorists try to foil the counter-terrorist surveillance experts by buying pay-as-you-go mobile phones which they use once and then throw away.

When it was alleged in 2004 that Kofi Annan, then United Nations Secretary-General, had had his offices bugged by American or British intelligence services, there was much speculation over whether the form of eavesdropping had been a planted mobile phone or an electronic bug.

However, there are other more sophisticated methods, including using laser technology. A laser beam bouncing off an office window can pick up the vibrations of conversation which can then be translated into speech.



Signs of the social networking times.

If you do not wish to receive any further Newsletters please contact Nick Graves by email.

This publication is intended only to provide a summary and general overview on matters of interest. It is not intended to be comprehensive nor does it constitute legal advice.

We attempt to ensure that its content is current but we do not guarantee its currency. You should seek legal or other professional advice before acting or relying on any of its content.



Looking after your future
Listening to your needs

Nick Graves
Phone: +61 2 9267 0661
Email: ngraves@corpsec.biz