



Technical Surveillance Countermeasures
Counter-Espionage Consulting

Client Briefing



ELECTRONIC SURVEILLANCE

Stop Bugging Me!

May 2010



Eavesdropping Aids...

Increasing Proliferation of Spy Products

Espionage devices (commonly referred to as spy products) have proliferated in availability and affordability both worldwide and within Australia. Spy products have become simple to install and function, and they are commonly being used to monitor keystrokes typed, intercept emails, log websites visited, copy documents opened, or monitor phone calls and text messages. An employee, or visitor to a target environment, can install any of the freely available spy products within a few minutes, in order to source confidential information. The resultant sale of confidential information to competitor companies or corporate intelligence practitioners causes the victim company vast financial, and reputational, damage. All organisations and their employees should be aware of the threat posed by espionage devices, which are no longer confined to the realm of professional spies and intelligence agencies.

Mobile Phone Espionage

Mobile phone espionage has become increasingly easy and affordable due to a significant rise in the number of Australian retailers offering mobile spy products and software. The problem has been exacerbated due to the rising number of phones offering advanced functionality such as internet access (which allows espionage software to be installed with ease). Mobile phone tapping received widespread media attention in mid-2009 after it was revealed that a major British newspaper had hired private investigators to tap the mobiles of several high-profile personalities across the sporting, entertainment and political spheres. Closer to home, the Sydney-based company, Spousebusters, came under the spotlight early in 2009 following their widespread promotion of mobile phone monitoring software. Meanwhile, Impact Investigations, also based in Sydney, offers mobile tracking services in which their clients log on to a website to track the target mobile phone's usage. Both companies have come in for criticism from government departments and privacy advocates.

Almost anybody is capable of using phone monitoring software to turn a mobile phone into a high-end surveillance device, without the need of any hardware applications. High quality mobile eavesdropping software can now be purchased for as little as \$400 in Australia and such software enables eavesdroppers to:

- ▶ Intercept, listen to, and record all phone calls (a SMS is sent to the eavesdropper's mobile each time the phone is used for a call).
- ▶ Listen to conversations even when the phone is not in use (i.e. the eavesdropper can remotely switch on the phones' microphone).
- ▶ Intercept incoming and outgoing emails and SMSs.
- ▶ View a phone's entire call history (including names of those called as per the phone's address book).
- ▶ Obtain the phone's precise location to within a few metres using triangulation.



Several mobile spy software packages only require an IMEI number in order to target a phone. The IMEI number, which can be easily found on the sticker under the phone battery, or by typing *#06# on the phone keypad, allows suitable tracer software to be created and installed in around five minutes. The target mobile's entire call and SMS records can then be easily viewed through web-based monitoring applications.

Other Widely Available Spy Products

A myriad of spy products are now available and are being widely used across Australia and the surrounding region. Several of the more commonly utilised devices include audio-recording USB drives, listening devices, vehicle location trackers and key loggers. This section details just a handful of the numerous espionage products that are now freely available for anyone to purchase and utilise.

USB sticks that also act as voice recorders can now be purchased in Australia for less than \$100. Such devices look and function just like any standard USB hard drive. However, a discrete on/off switch allows the USB drive to record up to 120 hours of conversation (for a 2GB drive). Such devices are silent and can be utilised whether they are connected to a computer or not. Other USBs also double as 'stealth phone recorders' and, after being installed in under five minutes, allow all incoming and outgoing telephone calls to be captured on any analogue telephone line. USB stealth phone recorders (less than \$300 when purchased in Australia) do not even have to be directed to the phone (they can just be connected to the same telephone line), and allow all calls to be saved onto a computer hard drive with the call's time and date recorded.

Increasingly efficient listening devices allow conversations to be listened to from a great distance. Such eavesdropping bugs can use several power sources, including telephone wiring, cable TV, or simply AC power circuits. However, many high quality listening devices only need minimal battery power to allow extended use (2 AAA batteries can power the continuous use of a listening device for around 100 hours). Eavesdropping bugs are frequently planted out of sight (often in voids and penetrations, amongst wiring, or attached to electronic devices) in company boardrooms and executive offices.

Several companies in Australia now advertise 'vehicle tracking services' whereby the precise, up-to-the-minute GPS location of the vehicle is monitored. Such devices are often about the size of two matchboxes and can be attached to the underside of any vehicle using a strong magnet. A SIM card inside the unit allows for an eavesdropper to be sent a text message with the exact longitude and latitude of the vehicle, with accuracy to within two metres. Such devices generally have long battery lives (approximately one week) and retail in the Australian market place for around \$900.

Key loggers come in a range of styles, from USB sticks, which do not require the installation of any software or drivers, to software-based products. These devices record all keyboard strokes and create stored copies of all written text. Advanced key loggers also allow all invisible keys (such as 'shift' and ctrl!) to be recorded, as well as details of which document the keys were typed into. Key loggers are often utilised within spyware applications (such as Trojan horses and viruses) to steal personal information such as passwords and banking details. Key loggers are widely available in Australia for around \$180 and normally allow over a year's worth of data (or two million keystrokes) to be recorded. The information is stored in a non-volatile memory, which retains the captured information even when the device loses power.



What Should You Do?

Jayde Consulting strongly advises our clients to invest in measures to reduce the security threats posed by the rapidly increasing range of spy products. The high number of spy products entering the Australian marketplace necessitates utmost vigilance on behalf of all personal with regards to security in the workplace. All employees should be informed about the potential threats posed by such devices and staff members should take precautions to minimise the risk of espionage devices being successfully placed. Employees should be encouraged to maintain a clean and tidy workplace, and to keep on the look out for suspicious devices around the workplace.

Mobile phone spyware is often hard to detect to the naked eye, and it is usually only accessible through pin codes installed by the eavesdropper. Changing the phone SIM card is generally of no use, as many mobile monitoring software packages offer SIM change notification features. Companies are advised to invest in security measures to help ensure that their employees' mobile phones are not jeopardized. Mobile phones should be kept within their owner's sight at all times and security passwords should be installed to help minimize the security threat. Removing a phone's battery can help to minimise the risk of eavesdropping occurring, although this is not a failsafe method. Signs that your mobile phone has been bugged can include an unusual drain on the battery and unexpected lighting up of the screen when the phone is not in use. However, many mobile espionage devices are almost impossible to detect, short of a forensic examination.

There are numerous security risks posed by USB portable hard drives, even if they do not have dual functionality as listening devices. Vast amounts of information can be stolen in a few seconds using such devices. Jayde Consulting recommends that companies should enforce a no-USB drive policy. Companies should closely regulate and monitor the downloading and transfer of confidential information and the use of personal emails in the workplace. Effective anti-virus and anti-spyware programs must be installed and regularly updated on all work computers to help minimise the risks associated with downloadable spyware.

Appropriate security measures will help to reduce the risks associated with spy products. Such security measures may include the enhancement of physical security procedures (including access control and CCTV coverage), tighter controls on the classification and management of confidential information and an ongoing employee security awareness program. It is essential that organisations ensure that all rooms where confidential meetings and discussions take place (in particular board rooms and executive offices) remain free of eavesdropping devices and other technical surveillance equipment. Jayde Consulting advises its clients that Technical Surveillance Counter Measures inspections should be regularly carried out to help ensure that sensitive discussions remain confidential. A whole realm of new security threats have emerged as the result of advances in network and communications technology. Cybersecurity involves the protection, monitoring and authentication of communications or online information against unauthorised access, use, modification and theft. However, the borderless and transient nature of the internet now allows criminal elements greater access to legal and illegal markets, money laundering, digital funds and the ability to circumvent both national and international laws and censors. There are an endless number of risks relating to cybersecurity and these include viruses that can erase entire computer systems, unauthorised access to alter company files, mobile phone hacking, keystroke logging, damage to network infrastructures and the theft of financial or sensitive information.



How We Can Assist

Jayde Consulting are professional counter-espionage consultants and assist a wide range of organisations, both in Australia and across the Asia-Pacific region, in the detection and deterrence of acts of espionage. Our team can ascertain whether an organisation or individual is the target of surveillance of espionage through an enhanced range of surveillance detection and technical surveillance countermeasures capabilities and the use of up-to-date technology equipment and processes. We have an experienced team of professionals available, whose sole focus is the protection of our clients' interests.

Furthermore, Jayde Consulting can provide advice and support on peripheral security measures that can be undertaken to reduce the likelihood of you or your organisation becoming the target of political, industrial or corporate espionage.

A proactive approach to security will assist in protecting your privacy, property and reputation.

All advice, services and consulting offered is on a strictly confidential basis. Our clients return to us, because they know that we will not discuss their cases with anyone. No exceptions. Integrity is paramount.

For further information on our counter-espionage services, please contact us via:

Website www.jaydeconsulting.com

Email contactus@jaydeconsulting.com

Telephone +61 [0] 2 8006 0635