

TECHNOLOGY

LEGAL UPDATE

SEPTEMBER 2005

CONTENTS	Identity theft: 'the evil twin'	01
	Spyware: who's watching you?	02

Identity theft: 'the evil twin'

Identity theft is not a new phenomenon. In fact, the provision of online services via the internet has made identity theft easier and more difficult to prevent. Improperly accessing and using personal records for the purposes of committing fraud is an ongoing IT security issue particularly for institutions like banks, financial services providers and government departments.

Key message

In a tight spot because of a hotspot? Finally there's a sin you can truly blame on your evil twin. But will that help?

Exploiting WiFi to access the internet

It's becoming more frequent for users of wireless computer equipment to use radio data communications systems such as WiFi to access the internet. The relatively small areas around each base station in which you can receive data are called hotspots. One of the latest mechanisms used to perpetrate identity theft involves attackers setting up unauthorised wireless base stations to create hotspots which appear to wireless users to be legitimate.

They do this by establishing a wireless access point near a legitimate base station by jamming connections to that access point and sending a stronger signal. An unwitting user will inadvertently connect to the attacker's unauthorised base station, believing he or she is accessing the legitimate network. With false login prompts, the user can unknowingly give away sensitive personal data, like passwords.

Base station cloning

The threat of base station cloning or 'evil twins', will become greater, particularly as public hotspots become more prevalent. Aside from the immediate costs to institutions like

banks, identity theft (such as 'evil twin' attacks) damages corporate reputations and may result in users rejecting cheaper on-line service provision.

Breaches of on-line security also expose corporations to increased liability. For example, a breach of on-line security measures may expose directors to claims that they have not complied with their common law and statutory duties to the corporation. In addition to breaching their common law duty, directors may be exposed to liability under section 180 of the Corporations Act 2001 which requires directors to exercise their powers with a reasonable person's degree of care and diligence. Furthermore, for listed companies, the Australian Stock Exchange's continuous disclosure listing rule may be contravened if the corporation conceals a breach of on-line security. Conceivably, a breach of on-line security is a matter which is material to share prices.

In the face of these threats, what measures can an organisation implement to address the technical and legal issues raised by identity theft like 'evil twin' attacks?

The most immediately apparent measure is to maintain and regularly update adequate technical security measures. For example, some Australian institutions have already instituted

two-factor authentication systems for online consumers. Bank cards are a common example of two-factor identification which involves two kinds of identification (usually a physical token, like a card, and another which is memorised, like a security code). Such security measures ensure that simply obtaining a password will not be sufficient for an attacker to access personal information.

Maintain an integrated risk management strategy

Simply relying on technical measures, however, will not be sufficient.

To minimise an organisation's legal exposure, it needs to develop and maintain an integrated risk management strategy. The integrated strategy should be developed by a combination of technical personnel, legal advisers and members of management. It should not only comprehensively deal with technical aspects of security, but also encompass issues like

customer education about on-line security. With increased dependency on external IT service providers and outsourcing, the strategy should also implement a contracting policy for third parties to ensure contractual responsibility and liability are appropriately allocated and distributed between the organisation, its service providers and customers.

Most importantly, the strategy should be subject to ongoing review and maintenance because as organisations respond to current on-line security threats, new ones will inevitably arise.

An organisation which has failed to take reasonable precautions may well explain with wide-eyed innocence to its aggrieved customer that, 'It wasn't me – it was my evil twin'. Just as with a mischievous child, that organisation is going to have a hard time making its case.

Cameron Abbott | Partner
Simon McDonald | Senior Associate

Spyware: who's watching you?

Key message

The federal government has initiated a legislative review in respect of spyware that will focus on the misuse of spyware technology rather than the technology itself.

What is spyware?

Spyware consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent.

Also commonly referred to as 'junkware', 'scumware', 'parasite software', and 'thiefware', spyware can sometimes be automatically installed simply by visiting a website.

Spyware is usually installed by one of three methods:

- » bundling – the spyware can come bundled with another program (commonly found bundled with P2P programs)

- » security flaws – the spyware takes advantage of security flaws in the internet browser
- » drive-by download – the browser installs the spyware on your computer via a download when you 'drive-by' a website (with or without any prompt, depending on security settings within the browser)

Once installed, spyware typically launches when a computer boots up and runs at all times, monitoring internet use and in some cases delivers targeted advertising to the affected computer.

Dangers?

Once installed on a computer, some malicious spyware can be used to monitor keystrokes, internet use and to obtain the credit card numbers or passwords of unsuspecting users. Spyware is commonly used by online criminals for purposes of identity theft and fraud.

Spyware can also siphon off bandwidth or processing capacity resulting in a slower internet connection. This type of spyware can also affect a computer's ability to run programs and in some instances can result in system crashes.

Perhaps the most common use of spyware is by online marketers. An affected computer is monitored, data is then transmitted back to the online marketer who then spams the user with relevant products.

Review of existing legislation

In August 2004, the federal government initiated a legislative review in respect of spyware. It was recognised that many beneficial and useful programs also use similar technology. The review focused on the misuse of spyware technology rather than the technology itself.

The review covered the following behaviours:

- » deceptive conduct
- » unauthorised access
- » cyber-stalking
- » computer hijacking
- » theft of computer software, resources and bandwidth
- » harvesting and collection of personal financial information
- » damage to computer settings
- » identity theft
- » internet banking fraud
- » content modification

- » browser hacking
- » anti-competitive conduct
- » invasion of privacy
- » impairment of security
- » cyber-harassment
- » denial of service attacks.

A number of existing laws were considered in the review including the Criminal Code Act 1995, the Trade Practices Act 1974 and the Privacy Act 1988.

In March 2005, the Minister for Communications, Information Technology and the Arts announced the outcome of the legislative review. The review found that the most serious and culpable uses of spyware are already covered under existing legislation.

Democrats 'Spyware Bill'

Despite the findings of the legislative review, there has been a continued push for new legislation to be passed specifically addressing the issue of spyware.

In early May 2005, the Democrats introduced into federal parliament their Spyware Bill 2005.

The proposed legislation is somewhat similar to existing spam legislation in that it does not propose to make spyware itself illegal. It will however require companies which use spyware to seek the permission of the user, to explain what information is being recorded and the purpose of using any such information. Companies will also be required to provide an easy uninstall feature for users.

The Bill proposes monetary fines and up to two years imprisonment for anyone convicted of installing spyware on a computer without the user's consent.

The second reading of the Bill in the Senate was adjourned.

Federal government's discussion paper

On 20 May 2005, the federal government issued a discussion paper seeking information and feedback from the Australian public to assist in developing practical responses that will target spyware in a way that does not constrain the use of beneficial or legitimate software.

The discussion paper emphasises that there is a wide range of software programs which possess similar components and capabilities to spyware that are both legitimate and of benefit to the user. Examples of this type of software include automatic security updates, remote administration tools and distributed processing.

The paper lists a number of scenarios describing how malicious spyware works, seeking feedback to specific questions and outlining possible responses to the problems caused by spyware.

Some of the potential areas of response listed in the paper are:

- » a legal framework that covers malicious activities associated with spyware
- » industry collaboration on best practices
- » availability of technical approaches to home and business users
- » consumer awareness
- » international cooperation to minimise the use or creation of malicious spyware.

Conclusions

Individuals and businesses rely more and more each day on the internet to shop, bank and conduct business. If spyware is not policed aggressively, it threatens to undermine the trust that computer users have in the online environment.

New legislation which specifically addresses malicious spyware would signal a determined approach to a serious problem which threatens the increasing use of the internet as a means of conducting business.

Despite the government's initial legislative review finding that spyware is covered by existing legislation, the industry will watch with interest any further submissions and proposals to combat spyware. If the Democrats' Spyware Bill is not passed, then the information and communication technology industry's response to the government's discussion paper may still influence the government to introduce its own spyware legislation.

Mark Feetham | Partner
Daniel Gleeson | Graduate

Further info

Cameron Abbott
Partner
T: +61 3 9640 4261
cameron.abbott@middletons.com.au

Mark Feetham
Partner
T: +61 2 9513 2540
mark.feetham@middletons.com.au