Schedule No.	Schedule Name	Brief Description
5	**Expert Determination Procedure**	Outlines the process for the determination of a dispute by an expert where an amicable resolution has not be achieved by the parties.
6	**Confirmation of Insurances**	A statement of insurances held by the Supplier.
7	**Financial Security**	A deed of agreement setting out the terms upon which a financial security is provided and may be called upon by the Customer.
8	**Performance Guarantee**	A deed of agreement setting out the terms upon which a performance guarantee is provided and may be called upon by the Customer.
9	**Deed of Confidentiality**	A deed of agreement setting out the terms for the preservation of confidentiality in certain information.
10	**Privacy**	Addresses the Supplier's privacy obligations.
11	**Escrow Agreement**	A deed of agreement between the Supplier, Customer and an escrow agent to place the source code of a product into escrow for release to the Customer in certain circumstances.
12	**Variation Procedures**	Provides a process for managing changes to the operational requirements of a project or variations to the terms.
13	**Risk Management**	Sets out the format of the risk management plan.

Who is spying on you? - taking a look at Spyware

Kylie Howard, Mallesons Stephen Jaques

Kylie Howard is a Solicitor in the Intellectual Property and Technology Group at Mallesons Stephen Jaques in Sydney and is also the editor of this journal. The article is based on a longer paper that was recently published in the Journal of Information, Law and Technology and co-authored by Yee Fen Lim, Associate Professor, Department of Law, Macquarie University: Howard and Lim, "I Spy with My Little Eye - Taking a Closer Look at Spyware" 2005 (2) *The Journal of Information, Law and Technology (JILT). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_2-3/howard-lim/*

What is spyware?

Spyware is a relatively new phenomenon. Spyware is intelligence gathering software that is both installed on a computing device and takes information from the computer without knowledge or consent of the user. Often the information obtained is given to a third party and used to build databases of information about people. It is called "spyware" because the software literally enables spying - it may target banking and credit card details, sensitive information, commercial information or your own private information.

A recent journal article discussing spyware opened with a statement that describes, in simple terms, the alarming nature of spyware:

> "You are being watched. Monitored. Every move you make is being recorded, logged. Your personal tastes and desires, your friends, travel plans, favourite TV shows, and newspapers. Perhaps more disturbing, this information is stored into databases, sold and shared with nameless and countless others. And you have no idea...."[1]

How a PC becomes infected with spyware and how do I know if my PC is infected?

A user of the Internet usually plays an unwitting role in downloading spyware, often by accident through downloading a spy-carrying email attachment, downloading "free" software[2] or simply browsing the Internet. Some examples of free software that have been known to be accompanied by spyware include browser toolbars and modifications, UnZip, PC clocks, personal organisers and Kazaa.[3]

Some spyware will use deception to mislead you into installing the software. For example, advertisements for "anti-spyware" tools may actually include spyware, or buttons that say "cancel" activate the installation of the spyware when clicked.[4] A user may even inadvertently consent to "monitoring" software as part of an end user licence agreement.

Although it can be difficult to know if your PC is infected with spyware, there are various symptoms that you should look out for. These include[5]:

- your computer's performance is slower than usual;
- error messages appear;
- new icons appear on your desktop that were not there before;
- new toolbars have been installed;
- your anti-virus and firewall software turns itself off;

- your web browser suddenly starts on a different home page;
- pop-up windows constantly appear;
- new pages in your favourites list;
- receiving large amounts of spam; and
- evidence of emails being sent from your computer without you sending them.

It may be a good idea to get an indication of whether your computer is infected. You can do this by checking:

- the "Add and Remove Programs" facility. This lists all the programs installed on your computer and is usually found in the main menu;
- the "task manager" to see which applications are running; and
- your firewall register for traffic between your computer and the internet.

Is it really an issue?

Many people think that because they have a firewall or virus protection software, they will be protected from harmful software such as spyware. This is not always the case. In addition, spyware is often deliberately designed to be difficult or impossible to uninstall.

There are some good reasons why spyware should not be tolerated. The main concerns with spyware include the financial costs involved with having spyware infected PCs, security issues and the right to privacy. Regarding privacy, in the offline world, would you agree to someone following you into shops, recording the purchases you make, looking at the types of books you read and then selling this information to a third party for marketing purposes? Probably not. In the virtual world, however, this is constantly happening - and not just to home users, but to companies as well. Some marketing companies are making millions of dollars selling personal information to third parties.[6] Specific concerns about spyware range from slowing down PCs to extreme invasions of privacy, not to mention the disruptive advertising pop-ups or the resources spyware can consume on a PC.[7] Companies have reported that they are losing millions of dollars in down time and lost productivity and expect the issue to get worse.[8]

Alarmingly, spyware is spreading at a very fast rate. Evidence of the worsening problem can be seen in a recent US survey (April, 2004) - over three months, some 30 million spyware programs had been installed on approximately one million computers. The number of spyware programs installed on a similar number of computers is now an alarming 85 million.[9] Other statistics include[10]:

- 80% of all PCs have been infected with spyware;
- 89% of infected users are unaware of the spyware found on their machines;
- 95% of infected users did not give permission for the software identified as spyware to be installed on their machines.

Spyware can be a serious security threat to your business and can be used for malicious purposes including[11]:

- secretly gathering information about a user and sending the information elsewhere;
- modifying computer settings and user preferences without the permission of the user; and
- stealing computer resources.

What legal protection exists against spyware?

It has been recognised that the availability of legal recourse against online offences increases the confidence of the public in using the Internet. In response to this, in 2004 the Minister for Communications, Information Technology and the Arts announced a review of the coverage of existing Australian laws in respect of the malicious use of spyware. The *Department of Communications, Information Technology and the Arts* ("**DoCITA**") began working with the Attorney-General's Department and law enforcement agencies to determine the adequacy of existing laws in combating spyware. DoCITA found that existing legislation, such as the *Criminal Code Act 1995* (Cth), the *Privacy Act 1988* (Cth), *Telecommunications Act* 1997 (Cth) and the *Trade Practices Act 1974* (Cth), covered many of the malicious behaviours associated with spyware[12] (this is explained in more detail below). The review covered behaviour such as deceptive conduct, unauthorised access, cyber-stalking, computer hijacking, theft of computer software, resources and bandwidth, denial of service attacks, damage to computer settings, identity theft, content modification, anti-competitive conduct and privacy infringements.

For the purposes of the legislative review, spyware was defined as:

> "any software application that is generally installed without the knowledge or consent of the user, to obtain, use or interfere with personal information or resources, content or settings for malicious or undesirable purposes".[13]

Table 1 (at the end of this article) outlines potential criminal offences that can be brought under existing legislation.

The Australian Democrats are of a different view to DoCITA. Their view is that separate legislation is required to specifically deal with spyware, and consequently the party has introduced *the Spyware Bill 2005* which is a proposed Act to regulate the unauthorised installation of computer software. It requires the clear disclosure to computer users of certain computer software features that may pose a threat to user privacy.

The objects of the proposed Act are to regulate the unauthorised or surreptitious installation of computer software and to require clear disclosure to computer users of certain computer software features that may pose a threat to a user's privacy or the speed or operation of their computer. The proposed Act aims to give computer users the right to know that software is being installed on their

computer, and the ability to refuse to have it installed and uninstall any software.[14]

Under the proposed Act consent by a user to install the software is designed as a two-step process with the requirement of an "affirmative consent", which must be expressed through the action of a computer user and is independent from any other consent solicited from the user during the installation process (for example, consent cannot be a broader consent for the installation of a separate software to which spyware is attached).[15] The first involves obtaining consent to the general installation of the software.[16] Secondly, consent must then be obtained for each individual information collection feature (and other features such as advertising, distributed computing feature and modification features) of the software. For example, if the spyware software once downloaded causes advertising pop-ups, collection of personal information and modifications to settings of the user's computer, the computer user must consent to each of these features before the software can be lawfully installed. This type of consent ensures that users are fully informed as to exactly how the software may affect them and their computer. Penalties under the proposed Act are directed to the actual software developers rather than passive parties such as the host of a website through which software was made available.[17]

On 1 September 2005, the Minister for Communications, Information Technology and the Arts, Senator The Hon Helen Coonan, released a media statement indicating that malicious uses of spyware are already covered by existing laws with an emphasis on the need for the public to be aware of the threat of spyware.[18] To complement the need for public awareness, DoCITA developed and released *Taking Care of Spyware*[19], a brochure designed to provide the public with information about spyware, how to remove it and how to prevent it. The brochure is supported by the Internet Industry Association's (IIA) national anti-spyware campaign[20] where the public can find more detailed information and sample the anti-spyware software that is available to use for a free trial period. Given this media release, it is unlikely that *the Spyware Bill 2005* will receive passage through Parliament. This may reflect the correct approach since it is questionable whether new legislation is the solution to the growing spyware problem.

Even if there was new legislation introduced in Australia that specifically covered malicious uses of software, that legislation would have a limited geographical field of application, with physical frontiers. It should be kept in mind that most spyware does not originate in Australia and so there are problems with asserting that Australian legislation will apply where spyware does not originate in Australia. For example, if a company in a jurisdiction other than Australia causes spyware to be installed without the relevant notices and consents that the proposed Australian legislation requires, does that legislation have any effect? It will all depend on whether Australia asserts jurisdiction over that company, and if it does, whether a judgment can be enforced in Australia. This very issue goes back to the widely debated topic of jurisdiction and the Internet. Existing legal regimes struggle to fit into the realm of the new Internet medium, and unfortunately, not much can be done except hope that other jurisdictions have similar legislative regimes and protective measures to cope with the various legal issues that have become as far-reaching as the Internet itself.

---

[1] Michael L Baroni, "Spyware Beware" 47-APR Orange County Law 36

[2] For example, the Kaaza file transfer program that was used by millons of people around the world to swap data also included another spyware software.

[3] Hon. Jefferson Lankford, "Big Brother is Watching You" (2004) 40-AUG Ariz. Att'y 8

[4] Internet Industry Association, Spyware Fact Sheet 2 www.iia.net.au

[5] Internet Industry Association, Spyware Fact Sheet 3 www.iia.net.au

[6] Commonwealth of Australia, Parliamentary Debates Hansard 2nd Reading Speech, 12 May 2005. "Companies such as Doubleclick make millions of dollars each year from the sale of data and the targeting of ads, yet their name is not often seen, other than in civil liberties courts."

[7] See http://www.adwarereport.com accessed 29 May 2005

[8] IDC, a company in the IT industry reported that $12 million was spent in 2003 on anti-spyware solutions. See http://searchsmb.techtarget.com/ accessed 29 May 2005

[9] Commonwealth of Australia, Senate Parliamentary Debates Hansard 2nd Reading Speech, 12 May 2005

[10] Statistics taken from AOL/ NCSA Online Survey October 2004

[11] Department of Communications, Information Technology and the Arts, "Outcome of the Review of the Legislative Framework on Spyware".

[12] See: http://www.choice.com.au/viewArticle.aspx?id=104706&catId=100245&tid=100008&p=1 accessed 5 June 2005

[13] http://www.dcita.gov.au/__data/assets/pdf_file/24939/Outcome_of_Review.pdf accessed 28 September 2005

[14] Clause 3, Spyware Bill 2005

[15] Clause 4 Spyware Bill 2005

[16] Clause 8(2)(a), Spyware Bill 2005

[17] See Clause 16, Spyware Bill 2005

[18] http://www.minister.dcita.gov.au/media/media_releases/taking_care_of_spyware_-_protecting_consumers_on_the_net accessed 28 September 2005

[19] http://www.dcita.gov.au/__data/assets/pdf_file/30866/05020018_Spyware.pdf accessed 28 September 2005

[20] www.nospyware.net.au accessed 28 September 2005

Table 1

Legislation	Potential offence
Criminal Code Act 1995 (Cth)	Attempting to commit a serious offence (such as fraud) using a telecommunications network; Unauthorised access, modification or impairment of data, information or programs with intent to commit a serious offence; Causing unauthorised modification of data, information or programs to cause impairment - including the reliability, security or operation of data, information or programs; Unauthorised impairment of electronic communication; Unauthorised access to or modification of restricted data - data held on computer and to which access is restricted by an access control system (such as passwords etc) associated with the function of the computer; Possession or control of information with the intention to commit or facilitate a computer offence; Producing, supplying or obtaining data with intention of committing or facilitating a computer offence; Dishonestly obtaining, possessing, supplying, using or dealing in personal financial information without consent; and Intentionally using a carriage service to menace, harass or cause offence.
Trade Practices Act 1974 (Cth)	Anti-competitive behaviour Misleading and deceptive conduct
Australian Securities and Investments Commission Act 2001 (Cth) and Corporations Act 2001 (Cth)	Misleading and deceptive conduct
Privacy Act 1988 (Cth)	Invasion of privacy Harvesting and collecting personal information
Criminal Law Consolidation Act 1935 (SA)	Identity theft
Telecommunications Act 1997 (Cth)	Applies to some use of personal information
Telecommunications (Interception) Act 1979 (Cth)	Collection of data and other information

The Medium, the Message, the Artist and the Image: unauthorised photography on the Internet

Katherine Giles, Arts Law Centre of Australia

Katherine Giles is a Solicitor at the Arts Law Centre of Australia (Arts Law). She advises artists and arts organisations around Australia on a range of legal issues including contracts, intellectual property, insurance, business structures, defamation and employment. Advice is given to arts practitioners and organisations working in all sectors: visual arts, music, literature, performing arts, community arts, film and multimedia. Arts Law is the national community legal centre for the arts, it was established in 1983 with the support of the Australia Council for the Arts.

Introduction

The medium, or process, of our time – electric technology – is reshaping and restructuring patterns of social interdependence and every aspect of our personal life...[1]

The unauthorised use of photographs on the Internet raises a number of interesting legal issues. This article will focus on a few of the issues raised by the Standing Committee of Attorneys-General discussion paper, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*