Title:
E-Privacy – Fact or Fiction?

Word Count:
384

Summary:
An article about e-privacy, the laws governing "spyware" or "malware"

Keywords:
spyware, malware, laws about spyware, e-privacy, eprivacy, EU E-Privacy Directive (2002/58/EC)

Article Body:
The Law Governing "Spyware" or "Malware"

The EU E-Privacy Directive (2002/58/EC) is aimed at modernising existing law in the area of e-privacy. Its focus is on the dangers of so-called “spyware” which, in extreme cases, can allow third parties access to your machine, storing knowledge of all kinds of information from the software on the system to user names and passwords. In essence, it allows someone you do not know to gain access to your confidential information, store their own information and also trace your activities.

Facilitate Disabling of "Spyware"

Whilst it seems that prior consent is not required from you in order to this, under the Directive a business must allow people to notify them that they do not want it. In simple terms, they must make it clear how to disable it. Furthermore, companies can only use such software for legitimate purposes and with the knowledge of the user.

Effectiveness of the Law

The problem with this is that the main offenders are people who will have little respect for the law and therefore policing it as a problem in the same way that the legislation allowing people to opt out of unsolicited marketing calls (the telephone preference service) has not been very effective due to the large use of such sales approaches by companies that are less than legitimate.

Best Practice

Our view, as solicitors representing the interests of businesses rather than individuals whose rights need protecting, is that even without the Directive the best practice is not to use spyware unless there are very compelling reasons to do so which add value to the end user in some form or other. It is not rocket science: the company wishing to acquire a good brand reputation will want to adopt a higher standard even than required by law if it is serious about building its brand.

Alternative Remedies

As an aside, for the more extreme cases of the use of spyware or “malware”, the Computer Misuse Act 1990 covers unauthorised access to computer material amongst other things and already makes this a criminal offence.

Core obligation

Under the Directive, service providers (ie. businesses) must inform individuals of the risk involved if they allow the spyware into their system. In essence, the bottom line message is: be transparent.

http://www.kaltons.co.uk