internet. In most instances, the user is presented a message on their screen, indicating the existence of the terms, a link to the terms and requiring the user to indicate their consent to the terms by clicking on an icon. The product cannot be obtained or the software downloaded unless the user clicks the icon, indicating their acceptance of the terms.

The Court characterised Netscape's agreement as a browse-wrap agreement. With these agreements, the internet site often simply refers to the existence of a licence agreement. Users are not required to view the agreement or indicate their acceptance of the terms before downloading the software or obtaining the product.

Impact on Australian businesses

In Australia, as in the United States, electronic transactions are governed by the general law of contract. It is likely that Australian courts will look to the United States for guidance when considering similar issues.

Businesses need to ensure that their on-line contracts satisfy the elements necessary to form a contract. As a general rule, the user should be immediately made aware of the full text of the license agreement and should be unable to proceed in downloading or using the software unless, and until, he or she assents to the terms and conditions. It should be obvious to the user that he or she is entering a contract with the you.

Finally, you should review the operation of your websites – if a user is unlikely to realise they are bound by the agreement, the terms may not be binding.

Update

Submission of the Legislative Watch SubCommittee of The New South Wales Society for Computers & the Law on the Cybercrime Bill 2001 (Cth)

The Senate Select Committee on Legal and Constitutional Affairs has adopted some aspects of the submission made to them by the New South Wales Society for Computers and the Law on the Cybercrime Bill currently before parliament.

The Cybercrime Bill, and its equivalent State legislation will form an extremely important part of the regulatory environment in the new economy. One of the key aspects of the Bill is the replacement of existing criminal offences by offences of causing unauthorised access to, or unauthorised modification of, data held in a computer, or any unauthorised impairment of the reliability, security or operation of any data held on any device used to store data by electronic means.

These provisions will have a critical application to such organisations as IT services companies conducting security audits or "white knight" hacks of their customers' systems and could arguably apply to such things as the application of virus checking software to email in transit.

The submission was put together by the Legislative Subcommittee of the Society.

The subcommittee's submission is available from:
http://www.nswscl.org.au/home/cybercrime.html

The Senate's report is available from:
http://www.aph.gov.au/senate/committee/legcon_ctte/cybercrimebill01/cybercrime_bill01.pdf