Casenote: EF Cultural Travel Bv -ats- Zefer Corporation and Explorica Inc

Dr. Adrian McCullagh Ph. D.(QUT), Freehills

Adrian McCullagh is a solicitor at Freehills in Brisbane and Adjunct Professor of Electronic Commerce Law at the Queensland University of Technology. He has degrees in Computer Science, Law (Honours) and a Ph. D in Electronic Commerce Law. Adrian was admitted to practice law in 1988 and primarily practices in IP, Electronic Commerce, Data Security, IT, and Telecommunications. He is a member of the Communications Information Advisory Board for the Queensland Government, board member of the Australian IT Security Forum, and Management Committee member for the ISRC at QUT. Adrian acts for numerous Federal, State and Local Government agencies and large corporations, particularly in the financial sector, in IT Security compliance, general IT contracting and large scale ICT Infrastructure Contracts.

A recent case in America highlights the need for adequate terms of use for public website owners and access control mechanisms.

On the 28 January 2003, the United States Court of Appeals issued a judgment concerning automatic access to publicly available websites that will have a far reaching effect, including websites located on Australian servers.

Background

Explorica and EF were competitors in the student travel arena. Explorica was formed by several former EF employees who believed that Explorica could compete by undercutting all of EF's prices for student tours. Explorica hired Zefer to build a 'scraper tool' that scraped pricing data from EF's website. A 'scraper tool', also known as a 'robot', is a computer program that automatically accesses information, contained in the HTML source code, in a succession of webpages. Explorica utilised the pricing data to undercut EF's prices by an average of five per cent. The district court at first instance issued a preliminary injunction against all defendants, including Zefer, based on one provision of the Computer Fraud and Abuse Act (**CFAA**), 18 U.S.C. §1030, ruling that the use of the scraper tool went beyond the 'reasonable expectation' of ordinary users.

Current appeal

The key issue addressed by the Court of Appeal was whether under the CFAA, Zefer had exceeded authorisation to access EF's public website by using the scraper tool.

The CFAA defines 'exceeds authorised access' as 'to access a computer with authorisation and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter'. The Court of Appeal noted that it is not uncommon for webpages to contain limiting conditions, such as limitations on the use of scraper tools. EF had no explicit prohibition on its website at the time of Zefer's use of the scraper tool.

The Court of Appeal considered the 'reasonable expectations' test adopted by the lower court to be unsuitable in the particular context particularly as use of the test is not prescribed by the CFAA. The Court of Appeal stated that a public website owner could quite easily state what is prohibited thereby avoiding the need to consider ambiguous standards like 'reasonable expectations'. The relative ease of including specific terms of use on a website was pivotal in the Court of Appeal's disapproval of the use of the imprecise 'reasonable expectations' standard.

Despite not agreeing with the district court's rationale for granting the injuction, the Court of Appeal did not vacate the injunction against Zefer for other reasons.

Application in Australia

The rationale exhibited by the United States Court of Appeal is equally applicable to the Australian environment, particularly considering the *Cybercrime Act 2001 (Cth)*. Section 478.1 of the Cybercrime Act makes it an offence to access restricted data without authorisation. 'Restricted data' is data to which access is restricted by an access control system. An access control system is any technology that regulates the access to a website. Therefore, a website requiring password registration may be considered as containing 'restricted data'. If the reasoning of the United States Court of Appeal is applied in Australia, any access prohibited by the terms of use would be considered 'unauthorised'. Thus, a person using a 'scraper tool' on a website with password access and clearly stipulated terms of use forbidding the use of scraper tools, would be accessing restricted data without authorisation and may be committing an offence under the Cybercrime Act. However, if no clear terms of use are displayed, it is doubtful any provisions of the Cybercrime Act will be invoced as the access to the website would not be unauthorised. Like the United States Court of Appeal, it is doubtful that an Australian Court would adopt a 'reasonable expectations' test.

Website owners should review their current website access rules an daccess control mechanisms so that they are better protected in light of this case.