What is "screen scraping" and is it lawful in Australia?

Trevor Jeffords, Freehills

Trevor is part of the Corporate Technology team at Freehills, Melbourne office. He has experience dealing with IT outsourcing agreements, web-development contracts, website linking affiliate agreements, web-based banking portals and general banking and litigation. Trevor is also an IT and website design lecturer.

What is screen scraping?

Screen scraping (or aggregation) is a method used to extract data from a series of webpages in order to consolidate that data on one central webpage. Companies that use this method are referred to as "aggregators".

Aggregation is used in many industries. For example, Bidder's Edge Inc. is a US internet auction aggregation site. The Bidder's Edge website allows users to search for items across numerous online auction sites without having to search each host individually. It does this via automated code robots which 'crawl' and 'scrape' data from the online databases of other auction sites.

In the banking sector, aggregators operate websites that allow customers to view their financial holdings at multiple financial institutions at a single location on the internet. Customers provide aggregators with their user names and passwords to all accounts they wish to see in one place on the internet. The aggregator uses this information to automatically access the customer's accounts, "scrape" the necessary data, and display this information to the customer in a consolidated form. Several account aggregators are currently operating in the US, such as Corillian, EZ Login, PayTrust, VerticalOne and Yodlee.

At present, the consolidated data displayed on most aggregators' websites is static and updates are conducted at regular intervals. However, this is likely to change as technology develops to the point where aggregator websites will be able to provide "live" data with the ability to send instructions - for example, an instruction to transfer funds direct to a financial institution.

Who loses out with screen scraping?

The service offered by aggregators is likely to be welcomed by many consumers because it enables them to conveniently view information sourced from a variety of websites at one single location. However, some companies who operate websites that have been scraped by aggregators have objected to the practice for various reasons, such as the potential diversion of custom from their website and the liability risks associated with data being extracted and possibly being corrupted or misused in circumstances which are beyond the control of the website owner. This raises the issue of whether an aggregator who scrapes information from a third party website needs to obtain the consent of the website owner. In Australia, it would seem that the answer to this question may be 'yes' on at least three grounds.

The first argument is based on state legislation which makes it an offence to access computer systems without lawful authority to do so. The second ground is based on the tort of trespass. The third ground is based on copyright law.

State Legislation

In each State of Australia, it is an offence to access a computer system without authority to do so. Taking Victoria and New South Wales as examples:

- Under s9A of the *Summary Offences Act* 1966 (Vic), a person must not gain access to, or enter, a computer system or part of a computer system without lawful authority to do so. (Penalty: $2500 or imprisonment for 6 months)
- Under s309(1) of the *Crimes Act* 1900 (NSW), a person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer is liable to imprisonment for six months or to a fine of $5000, or both.

It was argued during the debating of the amendments that created these laws that the unauthorised use of a computer system not involving criminal intent and harmful consequences should not be criminalised.[1] However this argument was rejected and at present, the laws of Victoria and New South Wales do not require fraudulent, criminal or malicious intent. Of course, as these statutes involve criminal offences, a successful conviction requires proof "beyond reasonable doubt" which is more stringent than the "balance of probabilities" threshold used for civil actions.

Trespass

It is well recognised that any unauthorised interference with goods in the possession of another constitutes trespass. However, it is unclear whether Australian courts will apply this traditional tort of trespass to an instance of unauthorised computer access. In the recent decision of the US District Court for California,eBay Inc -v- Bidder's Edge Inc,[2] eBay Inc was successful in obtaining an interim injunction on the basis of trespass which prevented Bidder's Edge scraping eBay Inc's internet auction website. In the US, it is necessary to show a likelihood of damage to succeed in an action for trespass. The court accepted that by using over 100,000 automated searches per day, Bidder's Edge Inc was "draining" eBay Inc's computer system resources away from legitimate customers and that this had caused some harm to eBay Inc. The decision has been criticised in the US on a number of fronts including on the basis that the harm to eBay was not in fact sufficient.

In Australia, on the other hand, it is generally accepted that damage is not required for a trespass to goods action to succeed; however, the monetary damage awarded by the court will be directly proportional to the loss suffered by the unlawful interference. Where the loss is minimal or non-existent, the court will only award nominal damages. The quantum of damage is probably not an issue however, for website owners who object to their websites being scraped. Their real remedy will be an order from the court injuncting the aggregator from continuing to trespass on the owner's website.

Copyright

In Australia copying data or substantially copying data from a third party website without the authority of the copyright owner may infringe s36 of the *Copyright Act* 1968 (Cth).

Issues which need to be considered here include:

- whether the data qualifies as an original "literary work" and is therefore capable of copyright protection; and
- who in fact owns the data - by way of example, where the data consists of the account information of a customer it might be argued that the data and any rights to the data is in fact "owned" by the customer and not the website operator.

Circumstances where consent to an aggregator accessing a third party website may be implied

The operator of a website will normally allow consumers to access and download data from the website for certain purposes. If all an aggregator is doing is accessing this data in its capacity as an agent for the consumer and the data is data specifically relating to the consumer (for example, the customer's account data), then the argument which can be run is that the aggregator's conduct is not in fact unauthorised. One risk with this argument is that the "scraping" of data by an aggregator (for example, because of the technical method in which the data is extracted) may go beyond the use which the consumer has been permitted by the website owner. The agency argument may also have less force where the data that is scraped does not specifically relate to the customer.

1 388 Vic. Parl. Deb. (L.C.) 470 (Hon. J. H. Kennan).

2 100 F.Supp 2d 1058

New legislation could make forwarding e-mails illegal!

Alison Lam, Freehills

The *Copyright Amendment (Digital Agenda) Act 2000* (**Act**) came into effect on 4 March 2001. Recent media reports have suggested that the Act could make it illegal to forward e-mails (even personal ones) to others. The reports suggest that such action could be construed as a breach of the copyright of the e-mail's original author. These reports have sometimes highlighted potentially hefty penalties of up to five years jail or $60,000 in fines.

In an effort to tackle these reports, the Attorney-General (**AG**) issued a news release on 4 March 2000 which labelled such assertions as 'ridiculous' and 'alarmist'. The AG stated that the Act is designed to update copyright law to ensure it provides the same protections in an electronic environment as exist in a hard copy environment. The Act allows copyright owners to restrain the unauthorised communication of their works to the public. The concept of "communication to the public" is intended to be technology-neutral and replaces the rights of a copyright owner to restrain the broadcast of their work and the transmission of their work to a diffusion service, whether in digital format or not.

The AG's news release states that forwarding a personal e-mail is unlikely to breach copyright laws since a court would need to find that the contents of the e-mail were an 'original literary work'. Most everyday personal e-mails were unlikely to satisfy this criteria. The examples cited by the AG included forwarding an old joke and a casual exchange of personal information or office gossip. Further, as some commentators have suggested, most e-mails are sent with an implied licence to use the e-mail in whatever manner might be considered normal practice. This includes opening, reading, printing and even forwarding them to other recipients.

Whilst some of the media reports have exaggerated the potential impact of the Act on e-mails, in some limited circumstances, forwarding e-mails may constitute an infringement of the copyright of the e-mail's original author. This is particularly so where an e-mail contains an express limitation on its further handling, such as an e-mail marked personal and confidential or where the content of the e-mail states or implies that it should not be forwarded to any one else. In addition to an action for breach of copyright, the original e-mail's author may also be able to sue for breach of confidentiality.

Ultimately, the test will lie in the value of the content of the forwarded e-mail. In practice most e-mails are unlikely to have an intrinsic commercial value which justifies an action for breach of copyright or confidentiality. It is only where e-mails have some intrinsic value and contain some limitation on their further handling, whether express or implied, that forwarding e-mails is likely to become a significant legal issue.

Can hyperlinks be prohibited?

Linklaters & Alliance Information, Technology & Communications

Hyperlinks are the main components of the World Wide Web (www). These links provide a connection between the contents of individual websites. They enable the user to "surf the net", i.e. change simply and quickly from one website to the next. Although it is thus the hyperlinks which give the www its network character, the use of such links has not yet been finally clarified. When examining this question from a legal perspective, a distinction must be made between the different technical types of link:

The basic link comprises a simple connection to the homepage of another website by referring the user to the third party Internet address (also referred to as surface-linking).

Until recently it was widely held that this kind of linking was unobjectionable. The Higher Regional Court of Düsseldorf, for example, held in its "*baumarkt.de*" judgment of 29 June 1999, that parties setting up websites must expect corresponding links to be made to their websites and thus are deemed to give their implied consent to such links.

The Regional Court of Hamburg took completely the opposite view in a recent decision on similar facts under competition law, in accordance with Section. 1 of the German Act against Unfair Competition (UWG). Here it was held that a website provider is not obliged to tolerate a competitor providing a link which leads users of the competitor's site directly to the website of the plaintiff provider.

This decision of the Regional Court of Hamburg appears dubious. In the absence of particular circumstances establishing the anti-competitive nature of a link there would not appear to be legal objections to a "simple" link if the objection is merely that the parties involved are competitors. However, the decision does serve to show the extensive range of possible interpretations and the uncertainty of the courts in trying to slot these new legal issues into the existing legal framework.

In contrast to the simple hyperlink, a "deep link", rather than merely connecting the user to the homepage of a third party website, leads straight "into the depths" of the third party site. This involves the user changing Internet addresses and the Internet user is or could be aware that he has changed sites.

So far the German courts have not expressly considered deep links. However, there is some support for the argument that deep links are actionable under Sections 1, 3 UWG.

First, the direct link can give Internet users the impression that the information belongs to the website containing the deep-link.

Secondly, a provider can cause damage to the third party provider - often a competitor - as this third party's Internet offers may, as a result of the link, be less commonly frequented. The frequency with which a website is hit is a criterion for judging the advertising effect of an Internet offer and thus the amount of advertising fees to be charged.

Framing also involves a link to third party content, with the difference that the Internet user will not necessarily recognise that this comprises third party contents, as the contents appear on the initial website within a separate "frame".

Framing does not involve a change in Internet address; the Internet user thus has the impression that he is still on the original website.

The Higher Regional Court of Celle decided in May 1999 that the use of third party information is unfair from a competition law perspective.

Framing involves a risk that Internet users will not directly access this provider's website as they can obtain same or additional information on the website of the first provider by way of framing.

Finally, there are doubts as to whether framing is compatible with copyright issues if the contents linked by the framing enjoy copyright protection. In such circumstances the Regional Court of Hamburg, in a judgment of July 2000 gave a remedy. Although a party providing a website must expect links to be made to its website, so that in principle it is deemed to give its implicit consent, this does not apply if activating the link does not cause the user to completely change to the third party website, with the result that the user could believe the offers provided on the linked website are offers of the party providing the framed link. In such cases one cannot assume that the owner of the intellectual property right in the second site has given its implicit consent to the duplication of its offers, in the form of a temporary storage of the website in the main memory of the user's PC.

A website operator wishing to avoid liability should obtain the consent of the operator concerned before providing a link to the other website, especially as more and more website operators are specifically refusing the activation of links without their consent.

(This article was supplied courtesy of Linklaters & Alliance Information, Technology & Communications Issue 11, May 2001)