Model Contract Clauses

Information, Technology & Communication, LinkLaters & Alliance News

The European Commission is preparing a model contract in relation to the transfer of personal data from the EU to countries without adequate data protection laws.

The model contract is expected to go to the European Parliament in March and to be approved by May 2001. It will be able to be used in a variety of circumstances including a transfer within an international group of companies and transfers amounting to licences for the use of data (for example, for direct marketing).

The model contract may not be as user-friendly as was hoped. Under it, a data importer will undertake to process personal data in accordance with the laws of the state of establishment of the data controller.

As there are differences in implementation of the EU data protection directive, this may result in administrative burdens.

(This article was supplied courtesy of LinkLaters & Alliance News "Information, Technology & Communications", Issue 9 January 2001

Web Bugs and Internet Advertising

Kaman Tsoi, Freehills

Kaman Tsoi is a solicitor in the Melbourne office of Freehills. He specialises in privacy, IT and e-commerce.

Introduction

"Web bugs" is one of the names given to an increasingly popular Internet monitoring device that has become a recent target of privacy advocates. Web bugs are most commonly found on the World Wide Web, where they are often used in conjunction with the more innocently named "cookies", as part of the tracking used in Internet advertising campaigns.

Because of the increasing integration of the World Wide Web with other software applications, it is also possible for web bugs to be planted in documents created using programs such as word processors. Often the process of linking the (invisible) web content into such a document happens without the user even being aware that the Internet is being connected to. Such web bugs could allow a document's author to track if, when and where the document is being read and how it is being passed on to different users. A similar technique can also be used to monitor written messages attached to forwarded emails. These uses of web bugs are still not widespread, and so this article will focus on the more common use of web bugs in the internet advertising context.

How do they work?

First, a quick primer on cookies. Cookies are small text files placed on a user's computer when a website is accessed, which allow that website to recognise the cookie when that computer is used to return to the website on another occasion. The cookie tells the website that "this is the same computer that was here last Wednesday", although it may not actually be the same user on that computer.

Web bugs are website graphics which serve the additional purpose of monitoring who is reading the web page. However, these "graphics" are often invisible to web users, as in many cases they are 1x1 pixel in size, with no border and the same colour as the page background. They are also known as "1-by-1 GIFs", "clear GIFs" and "invisible GIFs".

This should make more sense if we get straight to an example. Our four players are the advertisers (the companies that wish to advertise their products and services on third party websites), the ad hosts (whose websites display the ads), the network advertisers (who act as intermediaries between the advertisers and ad hosts) and, of course, the internet users.

Let us say a user accesses an ad host's home page. That page would contain the ad host's own content, as well as content in the form of a banner ad which is automatically served to the ad host's home page from a network advertiser's server. The banner ad would advertise the products or services of an advertiser and, if clicked on, would usually link to the advertiser's website. In this example

there may be direct relationships between the network advertiser and each of the ad host and the advertiser, but not necessarily between the ad host and the advertiser. The user may have no prior relationship with any of the other parties. But when the user views the ad host's home page, in addition to any cookie which may be set by the ad host itself, the network advertiser serves a cookie to the user's browser. And because the banner ad graphic is operating as a web bug, the network advertiser receives information including the IP address of the user's computer, the URL of the ad host's home page, the time that the page was viewed and the type of browser being used by the user.

If the user then clicks on the banner ad to link through to the advertiser's website, the further movements of that user would be monitored to the extent that the network advertiser had invisible web bugs on any pages of the advertiser's site. Each time a web bugged page is viewed by the user, the network advertiser receives the same information about the IP address, page URL, time and browser type, along with the cookie value that was set when the banner ad was first viewed. Unless the user deletes the cookie, this monitoring could occur even if the user did not view the advertiser's site immediately or via the banner ad link. This sort of tracking allows advertisers to gauge the effectiveness of different advertising campaigns, by measuring not only how many users follow the banner ad through to the advertiser's site, but even how many proceed further into the advertiser's site to an online purchase or registration which may have been the primary aim of the advertising. Depending on how the web bugs are set up by the network advertiser on the advertiser's website, the reports which are generated by network advertisers can show advertisers the exact point at which users drop out of the picture, whether it is by not going any further than viewing the ad host's page containing the banner ad, or at some preliminary point on the advertiser's website prior to ultimate purchase or registration.

While this is all impressive, particularly in comparison to other forms of advertising, what really takes web bugs into mind-boggling territory is simply this: for each network advertiser, there are many more ad hosts, advertisers and users. What this means is that by using the same cookie wherever the network advertiser has banners or web bugs on ad host or advertiser sites, the network advertiser can consolidate the data related to a particular cookie to form a detailed profile of browsing habits which could include the types of sites visited. The network advertiser can then add value to its advertisers by using these cookie profiles to determine what ad is shown the next time a user with that cookie is identified visiting an ad host's site. The major network advertisers hold hundreds of millions of these consumer profiles between them. The AltaVista search engine can be used to search for web bugs, and one recent search reported more than four million web bugs planted by 30 vendors on the internet.[1]

Cookies do not necessarily mean that personal information is being collected and used, however there is certainly potential for cookies to be linked to personal information. One method is to send HTML email messages which themselves contain web bugs that serve cookies. This allows an association to be made between the cookie and the email address. Any further browsing of websites in the ad network could then be tracked to develop a profile which could be matched to the email address, which may then be the target of marketing messages tailored to that browser's profile.

Privacy concerns

Clearly, many of the practices I have outlined have privacy implications which have already raised the concern of consumers and privacy groups. High amongst these is the fact that the use of web bugs is often invisible. In many instances the website user has no idea of the network advertiser's presence or identity on a website, nor of the placement of cookies to track browsing activity within and across multiple websites, nor of the targeting of advertising to their browser.

Under the recently passed amendments [2] to the Privacy Act 1988 (Cth), which will extend the effect of that Act to the private sector from 21 December 2001, the issue will be whether the use of web bugs involves "personal information", that is information about an individual whose identity is apparent, or can easily be ascertained, from the information. In many cases companies may argue that information collected using web bugs and cookies is aggregated information which does not identify individuals.

While this argument may sometimes be correct, it should not be made without considering the following issues.

First, while the cookie ID may not ever collect personal information or be linked to personal information – so the user's identity is never known – the use of the information, such as targeted advertising, may nevertheless relate to an individual. Whether or not this is addressed by privacy legislation, it is something that many consumers would consider relates to their privacy, and so may be a public relations issue rather than a legal one. While for some, targeted advertising is relatively benign, commentators have suggested that the profiles developed with the use of web bugs and cookies could be used to determine the prices and terms a particular user sees when shopping online for goods and services, including services like life insurance.

Secondly, the use of web bugs and cookies by network advertisers may involve the collection of personal information from an advertiser's website, without any deliberate disclosure of that information by the advertiser, perhaps without the advertiser even being aware that it is happening. One way that this could happen is where the URL or internet address of a web page contains personal information, and the URL is automatically sent to the network advertiser via the cookie. The sort of web pages where this may occur include pages around surveys, registration and purchase, particularly where a page reproduces previously entered personal information for confirmation or some other purpose. In the same way, it is possible for network advertisers to track query terms entered in search engines.

Thirdly, because network advertisers will often use the same cookie wherever their web bugs appear across their entire network of ad host and advertiser websites, the network advertiser may know the identity of the individual to whom the cookie relates. Once they have made the association between the cookie ID and the person, the network advertiser can link any of the other information collected by the cookie to that person's profile. As I have outlined earlier, there are a number of opportunities for network advertisers to make this association, including by sending a web-bugged HTML email, receiving personal information from a cooperative site in the network or receiving personal information in URL strings, as outlined in the previous paragraph.

US responses

The Federal Trade Commission (**FTC**), which has been a key player in online privacy in the US has overseen draft proposals for self-regulation by the Network Advertising Initiative (**NAI**), an organisation made up of the leading internet network advertisers. Under the NAI Principles,[3] network advertisers agree to abide by the Guidelines for Online Privacy Policies set out by the Online Privacy Alliance[4] Those Guidelines expand on the privacy principles of notice, choice, access, security and data quality.

The NAI Principles go further in addressing specific issues relevant to the internet advertising industry. Network advertisers are required to take steps to ensure that users are given notice of online profiling activities on ad host and advertiser websites. This will be done by contract where a contract exists with the network advertiser, however the network advertisers do not always have a direct contractual relationship with third party websites on which the network advertisers collect non-personally identifiable information. A higher level of notice is required where personally identifiable information is collected. The NAI Principles also deal with the particular situations in which opt-in and opt-out consents are required from consumers before the network advertisers can engage in those online profiling practices.

While the NAI Principles have been a significant step towards greater privacy protection in the sphere of internet advertising, the FTC still recommended that US Congress enact legislation to protect the privacy of users in relation to online profiling.[5] Already there are a number of bills before both Congress and the Senate relating to online privacy [6] and the bipartisan Congressional Privacy Caucus recently held a briefing for relevant experts to present on the specific issue of web bugs.[7]

In February 2001, seven network advertisers announced that they have joined a program under which Arthur Andersen will manage compliance with the NAI Principles.[8] The program includes provisions for complaints, audits, investigations, sanctions and notice by Arthur Andersen to the FTC of a failure to comply. At the date of writing, the FTC is considering details of this compliance program, as well as a mechanism allowing internet users to use the NAI website (www.networkadvertising.org) to opt-out of the targeted advertising practices of each participating network advertiser.[9]

US states have also been looking to impose restrictions on the use of web bugs. In June last year, the US state of Michigan served notices of intended action against 4 high profile websites, saying that their privacy policies were inadequate as they did not disclose the use of web bugs on their sites.[10] The sites all agreed to amend their privacy policies in response to the notices, which alleged that they had violated Michigan's Consumer Protection Act by failing to fully disclose material facts about their information-gathering practices. The Act requires companies to truthfully disclose all relevant and material information regarding a transaction.

Australia

Could this happen in Australia? While our Australian Competition and Consumer Commission, (which oversees the Trade Practices Act 1974 (Cth)), has not been very active to date in the field of privacy, there is certainly potential for misleading and deceptive conduct to occur in this area. Clearly, where there is direct inconsistency between what is stated in a privacy policy and the actual privacy practices of an organisation, this could amount to misleading and deceptive conduct. This is one reason why it is important for companies to always ensure that their privacy statements are kept up to date with their current practices. While the Trade Practices Act does not have any equivalent provision to Michigan's Consumer Protection Act requiring companies to truthfully disclose all relevant and material information regarding a transaction, it is possible for silence to amount to misleading and deceptive conduct where there is a duty to disclose relevant facts. It could be argued that by making web bugs invisible, users may be misled to believe that their web movements are not being tracked.

One minimal way to reduce the risk of web bug use being found to be misleading and deceptive would be to disclose the use of web bugs in a website's privacy policy. This would also go towards compliance with Australian Privacy Laws. Ideally, opt-in and opt-out mechanisms should be available for users to have choice in relation to the information collected about them using cookies and web bugs.

In addition, where any personal information is disclosed to network advertisers via web bugs or cookies, organisations will need to consider the impact of the (National Privacy Principles (**NPPs**). The NPPs set out guidelines for the fair handling of personal information and deal with such issues as collection, use and disclosure of personal information. A particular NPP of relevance to the present situation is the principle relating to "transborder data flows", since the majority of the internet advertising industry is based in the US. In many cases, to comply with the NPPs, companies whose network advertisers are based overseas and who collect or analyse web bug data containing personal information, would need to have a reasonable belief that the network advertiser is subject to a law, binding scheme or contract

which effectively upholds privacy standards substantially similar to the NPPs. If the network advertiser is subject to the Arthur Andersen compliance program for the NAI Principles, then it is arguable that those NAI Principles are substantially similar to the NPPs given that they contain requirements which broadly parallel the NPPs relating to collection, use and disclosure, data quality, data security, openness, access and correction and sensitive information. While the compliance program to be managed by Arther Anderson is still awaiting finalisation, current indications are that it will be a "binding scheme" and so satisfy one of the requirements of the NPP relating to transborder data flows. In other cases where no relevant law or binding scheme applies, this NPP could be satisfied by incorporating terms relating to privacy into an agreement with the network advertiser.

In November 2000, a Senate Select Committee on Information Technologies released its report entitled "Cookie Monsters? Privacy in the Information Society". Amongst its recommendations was one that the definition of "personal information" in the Privacy Act should be amended to extend to information that could indirectly identify an individual.[11] This recommendation was made in light of the possibilities for linking individuals to information collected by the use of web bugs and cookies. While at this stage there is no indication of whether this recommendation will be adopted, the degree to which companies fail to adopt good privacy practices in the interim may determine if and when the scope of the Privacy Act is further extended.

1 Richard Smith, "Invasion of the Web Bugs", 28 February 2001,

http://www.privacyfoundation.org/commentary/tipsheet022801.html

2 Privacy Amendment (Private Sector) Act 2000

3 Network Advertising Initiative, Self Regulatory Principles for Online Preference Marketing by Network Advertisers, July 2000,

http://www.networkadvertising.org/press/principles.pdf

4 Online Privacy Alliance, Guidelines for Online Privacy Policies,

http://www.privacyalliance.org/resources/ppguidelines.shtml

5 Federal Trade Commission, Online Profiling: A Report to Congress - Part 2, Recommendations, July 2000,
http://www.ftc.gov/os/2000/07/onlineprofiling.pdf

6 For example US House of Representatives, 107th Congress, Session 1, H.R. 89: Online Privacy Protection Act of 2001, sponsored by Rep. Rodney Frelinghuysen (R-NJ); US House of Representatives, 107th Congress, Session 1, H.R. 237 Consumer Internet Privacy Enhancement Act of 2001, sponsored by Reps. Anna Eshoo (D-CA) and Christopher Cannon (R-UT); US Senate, 107th Congress, Session 1, S. 30: Financial Information Privacy Protection Act of 2001, sponsored by Sens. Paul Sarbanes (D-MD), Patrick Leahy (D-VT), Christopher Dodd (D-CT), Jack Reed (D-RI), John Kerry (D-MA), Tom Harkin (D-IA) and John Edwards (D-NC).

7 Joe Barton and Ed Markey, "Has Your Email Been Bugged? Is Someone Monitoring What Web Sites You Visit?", 26 February 2001,

http://www.house.gov/markey/markeybartondc.pdf

8 Network Advertising Commission, Seven Internet Advertisers Join NAI Self-Regulatory Compliance Program to be Operated by Arthur Andersen, 1 February 2001, http://www.networkadvertising.org/NAI_PR_Feb1.pdf

9 Ibid

10 Michigan Office of the Attorney General, Summary of Notices of Intended Action, Alleging Inadequate Privacy Policies, Issued to Four Web Publishers on June 12, 2000, By Michigan Attorney General Jennifer Granholm,

http://www.ag.state.mi.us/AGWebSite/consumer_and_business_info/nia_612_s.pdf

11 Senate Information Technologies Committee, Cookie Monsters? Privacy in the information society, November 2000, Commonwealth of Australia 2000, p 4.