Growing concern over Internet privacy

Mike Ingram
25 February 2000

A number of lawsuits currently underway in the US have drawn attention to privacy issues raised by the use of “cookies” or strips of data sent to an Internet user's browser by a web site.

The cookie technology was developed to make browsing the Internet a more personalised and interactive experience. It is used on numerous web sites to deliver personalised content or track a user through an online shopping cart. The cookie is a small file stored on the user's hard drive for later retrieval upon subsequent visits to a site or a network of sites.

Privacy campaigners assert that they are being put to more sinister use by a number of leading Internet companies.

Among the more sensational is a case filed by a Texas lawyer against Yahoo! Inc. and a company it owns called Broadcast.com.

Lawrence J. Friedman filed the case last week in the Dallas District Court. It seeks class-action status on behalf of 50 million Yahoo users in the United States and seeks economic damages of more than $50 billion for violation of the state's anti-stalking law, together with other charges including theft of property.

Friedman is claiming that Yahoo's use of cookies is a “surveillance-like” scheme that monitors and stalks users without their consent or full knowledge. The named plaintiff in the case is Karen Stewart, a resident of Tarrant County, Texas. Friedman has not said why she was chosen.

A lawyer acting for Yahoo has vigorously denied the allegations, calling it a case of “very creative” legal theory that “seems to be completely off the base.”

By itself, cookie technology does not identify individual users. It simply records the movement of a particular browser on a specific computer as it visits a web site. By keeping track of which pages are viewed from the browser, web sites are able to offer customised content, most specifically, targeted advertising.

It seems unlikely that Friedman's case will stand up to scrutiny as the stalking laws are designed for the personal protection of individuals. Yahoo! maintains that its cookies do not identify an individual but a computer.

Several more credible lawsuits have been mounted, leading the US Federal Trade Commission (FTC) to investigate a number of web sites and Internet companies.

A number of health care web sites are under investigation over allegations that they shared personal information collected from consumers with other companies without proper warnings. The investigation follows a report by the California HealthCare Foundation, which denounced online health care sites for sharing information given by consumers with third parties despite promises that no data would be passed on.

The report, released February 1, was based on a survey of the information gathering practices and privacy notices at 21 web sites. “At best, the privacy policies of health Web sites are confusing, inconsistent, weak and often misleading when measured against the sites' actual practices,” the reported stated.

The use of technology to aid market research for the benefit of the advertising companies is not new. Anyone shopping in high street stores using a credit card is leaving a foot path for the advertising companies to follow which is far more clearly marked than those set by cookies on the Internet. Moreover, supermarkets and the like have been selling databases of customer shopping habits to third party companies for years, through the use of discount cards and bonus point schemes. As with the Internet cookie, no prior consent is sought. Invariably these databases include not only what was bought, but by whom, including information such as addresses and telephone numbers.

One company that has become a favourite for attack by privacy advocates is DoubleClick. This is by far the biggest Internet advertising agency and places ads for its clients on about 1,500 web sites—including some of the most heavily used sites such as Alta Vista—that are part of the DoubleClick network.

DoubleClick uses cookies to place a small file on a computer user's hard disk, which carries a special identifying number. The cookie allows DoubleClick to monitor the user's computer but the company can't identify the user by name or address. Whenever the user visits a site on the DoubleClick network, DoubleClick are able to note the content they are viewing to deliver a targeted advertisement

that is customised to the user's interests.

Founded in 1996, DoubleClick built its business plan around anonymous tracking. But at the end of last year it acquired Abacus Direct for a price of $1.7 billion in stock. Abacus builds databases of millions of names and addresses. The merged companies have launched a program called Abacus Alliance, which will collect names and addresses of Internet users. This data can be used to target them for both online and postal advertising.

On Thursday February 17, the State of Michigan gave a “notice of intended action” to DoubleClick, warning that the company has ten days to “cease and desist” the activities that the state finds unlawful, or else the Michigan Attorney General's office will file suit.

The notice alleges that the company secretly places cookies on the computers of people browsing the web sites in its network, knowing that the user is unaware that this is being done. “In reality, most consumers have not been given notice, have not knowingly consented to or authorized the placement of surveillance cookies, and are unaware of DoubleClick's opt-out policy”, the notice says.

The notice also alleges that DoubleClick changed its own privacy policy without adequately informing consumers.

The present privacy notice says the following:

“The non-personally identifiable information collected by DoubleClick is used for the purpose of targeting ads and measuring ad effectiveness on behalf of DoubleClick's advertisers and Web publishers who specifically request it...

“However, as described in ‘Abacus Alliance' and ‘Information Collected by DoubleClick's Web Sites' below, non-personally identifiable information collected by DoubleClick in the course of ad delivery *can be associated with a user's personally identifiable information* if that user has agreed to receive personally-tailored ads.” [emphasis in original]

It is the possible association of the information collected by the cookie with personally identifiable information that privacy advocates oppose most strongly. Not only could this lead to web users getting flooded with junk mail and online advertising, information gathered by health sites and others could be used against users in other walks of life such as when applying for jobs.

In theory everyone has a choice not to receive cookies. Security settings in the two most popular browsers, Netscape and Internet Explorer, allow the user the option to block all cookies, to be prompted upon receipt or to allow all cookies to be received. In practice however, most computers come with browsers installed with the minimal security settings and few users think to change them. Moreover, if a user has the option selected to “ask before accepting cookies,” the message which appears on screen says that the page may not be viewed correctly if the cookie is refused.

The concerns raised over the commercial use of information gathered by Internet companies such as DoubleClick are entirely legitimate. Even more serious questions emerge however when one considers how the security services and government agencies might use this information. This technology allows such agencies to track a user's political activity through monitoring both the web sites they visit and any discussion groups they may participate in.

Documents disclosed in September 1997 revealed a plan for the creation of a national identity database for the federal government. New Hampshire based Image Data held a contract worth $1.5 million with the US Secret Service to begin digitising existing drivers' licenses, photos and other personal data and feeding it into a national database.

Using a technology called True ID, Image Data fed information into its database in one of two ways. The company held contracts with state motor vehicle departments that supplied negatives or digital images on magnetic tape. It also persuades shoppers to scan their IDs into the database by inserting them into devices at specially equipped stores.

When the pilot scheme became known, the governors of Colorado and Florida halted the transfer of images to Image Data, and South Carolina filed suit asking for the return of millions of images already in the company's possession.

Through systems such as the Abacus Alliance set up by DoubleClick, the security services will have access to a massive database of millions of people with only the minor convenience of requiring a warrant.