What will the EU's stance on Internet cookies mean for web site operators?

Tough cookies

WHAT THE LEGISLATION SAYS

The proposed 'ban' on cookies under consideration by the European Union is based on a report on data protection drafted by Italian MEP Marco Cappato. Among other things, it proposes that article 5.3 of the EU's data protection guidelines be amended to read: "So-called cookies, spyware, web bugs, hidden identifiers and other similar devices that enter the users' terminal equipment without their explicit knowledge or explicit consent in order to gain access to information, to store hidden information or to trace the activities of the user, may seriously intrude on the privacy of these users. The use of such devices should therefore be prohibited unless the explicit, well informed and freely given consent of the user concerned has been obtained."

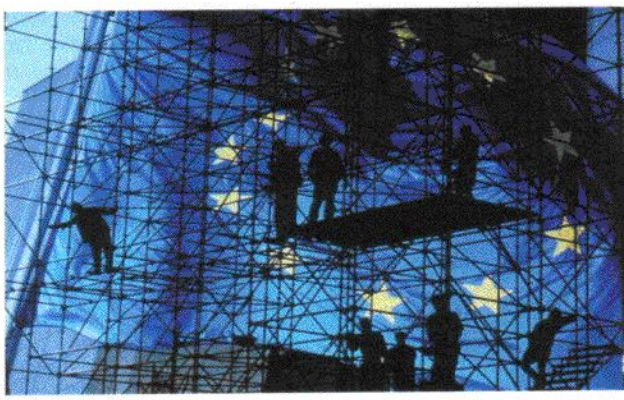
The EU's threat in October 2001 to ban 'cookies' surprised and upset the world of ecommerce. Although many people believe cookies to be the tools of malicious web site owners intent on spying on their customers, these small files of data are usually put to far less insidious uses. So is the European Parliament wrong to believe that the use of cookies has privacy implications, or is this just another example of technically illiterate politicians passing laws to prohibit technologies they do not understand?

Cookies were invented by browser company Netscape, which needed to overcome the then 'stateless' nature of web traffic. Servers could not easily tell whether a request for data came from the same computer and person as previous requests. The company's solution was to temporarily store an identification number in a file on the browser's computer that the server could ask for with every request for data. As a result, servers could differentiate between requests and ensure that re-authentication was not needed every time.

These 'session cookies' are temporary and disappear when the browser leaves the site, but Netscape and other companies saw the value in having more permanent cookies that they could use for personalisation of sites and for persistent authentication between sessions – particularly useful for customers with dial-up connections who are unlikely to have the same Internet address twice.

Since the invention of cookies, many people have worried about what information companies might store on them – and what they might do with it. Subsequent examples of companies abusing people's privacy using cookies (see box, *When cookies turn bad*) have made them seem a universally bad idea.

As a result, while virtually all browsers support cookies, most of them offer users the option to decline them as well. But this capability is rarely precise: only the less well-known browsers, such as Opera, Konqueror for Linux and iCab for Mac OS, have traditionally given users the ability to switch off cookies from specific sites for specific periods of time, or to carry out other pieces of fine tuning. Most browsers have a blanket option to accept cookies, to ask before accepting or to automatically decline cookies: anyone who has visited a series of web sites, only to be prompted for a cookie ten times and to find all their personal information is forgotten, usually resets the preferences back to automatic acceptance in no time. It is only since the release of Internet Explorer 6.0 that a mainstream browser has given the user any real degree of control over cookie-acceptance.



Since the invention of cookies many people have worried about what information companies might store on them – and what they might do with it.

Jon Paul Nollmann, chief security officer of online advertising network AdAce, argues that cookies are a shortcut taken by programmers that is almost never necessary and can be used to invade privacy. He believes that cookies are only necessary when passing information between otherwise separate sites – in other words, tracking users. "The only function provided by cookies that can't be done in any other way is 'frequency capping'. If you have bought a big ad campaign with a lot of impressions and don't want one user to see the ad more than three times, say, you need to track how often they've seen a particular campaign. When the campaign is running across at least two unrelated websites, the ad servers have to create and manipulate a cookie to track this." Every other current use for cookies, he maintains, "can be done better without them, or shouldn't be done at all".

For Nollmann, the security case against cookie use is clear: Even if not intended by the web site for mali-

cious purposes, cookies can be subverted and so always represent a potential risk to privacy. "I am strongly opposed to the use of cookies in any situation where some other method is possible. As chief security officer of AdAce, I've put my foot down on this issue: no cookies where we can do something else, and even if we can't do something else, no cookies if it's possible for it to be exploited by acquisition, mismanagement, or subpoena, to violate someone's privacy." He points to a whole range of past security alerts in which hackers were able to develop web pages that exploited bugs in browsers to reveal the personal information stored in cookies, or even steal them, so that they could masquerade as the cookies' owners. For him, cookies are too much of a privacy risk to be used with confidence.

MISUNDERSTANDING

Rufus Evison, chief technology officer of web measurement specialist ClickStream Technologies, believes that much of the concern is founded on a misunderstanding of cookie technology. "People think of cookies as little programs put into every web page that then get downloaded onto your computer, but they're just an item of information that remains."

Without cookies, ecommerce shopping baskets, web site personalisation and even some online games would become far harder to program, he says. And the more advanced features of Clickstream's cookie-based user monitoring systems – which include monitoring how a customer interacts with cached pages while they are offline – would be impossible to accomplish without forcing users to download a plug-in, something that has far more privacy concerns than a cookie, he argues.

Evison says the biggest problem with restricting the use of cookies as the EU plans is not that it is impossible to work without them; the far greater problem is redesigning existing sites in the current commercial climate. It would be far easier and cheaper for most companies to host a site overseas than to redesign their sites to work without cookies. He is even aware of some organisations saying they will ignore the EU ruling, because their site cannot function without cookies, and they will never be able to justify the cost of a rewrite: it will be easier just to hope no one spots that their site fails to comply with the ruling.

With privacy issues high on the news agenda, how companies use cookies is likely to become a more widely discussed issue than the possible consequences of their misuse. But many organisations may decide that the fear of cookies and the legal ramifications of failing to highlight their use, coupled with more sophisticated browsers offering users the option of circumventing cookies, are factors too significant to be overlooked in their ecommerce strategies.

WHEN COOKIES TURN BAD

Online advert provider DoubleClick is the most notorious user of cookies. The company serves ads to web sites from its own servers, giving advertisers a central source from which to buy adverts, while collecting data about how many times the ads have been displayed and how many customers have clicked on them. Web sites that have DoubleClick adverts on their sites insert code provided by DoubleClick into their pages and the ad appears automatically. However, the code is not simply just a call for an image: it is a JavaScript program that also places a cookie on the browser's computer.

DoubleClick aroused the ire of Internet users in 2000 when it emerged that the company was gathering all the information it had obtained from ads on different sites and correlating that with the identification data it had placed in the cookies. The company was able to track individual users, identify which sites they had been to, and determine their interests so that it could target certain adverts at them. The public outcry that ensued forced DoubleClick to abandon these practices and to stop tracking users.

The company has had to go one step further with the introduction of Internet Explorer (IE) 6, which by default stops third-party cookies (those placed on a computer by a site other than the one being browsed) and alerts users unless the third-party has a privacy policy that complies with the World Wide Web Consortium's Platform for Privacy Preferences Project (P3P) standard. According to management consultancy PricewaterhouseCoopers, 12% of US web surfers have started to use IE 6 since it was released in August 2000, so DoubleClick (in common with almost all third-party advertisers) had to audit its use of cookies and data to develop a P3P policy quickly.

DoubleClick's chief privacy officer Jules Polonetsky says he and his engineers began preparing for IE 6.0 at the start of 2001. The audit took "hundreds of hours" and also forced the company to spell out its policies for data storage and sharing. P3P mandates that an independent third party verifies that the company is abiding by its privacy policy, so for now, DoubleClick is off the hook as far as most web users are concerned.

CONTACT
Rob Buckley **rbuckley@infoconomy.com**

WHAT NEXT FOR THE LEGISLATION?

In October 2001, the EU Citizen's Freedoms and Rights, Justice and Home Affairs Committee approved the 'anti-cookie' amendment to the EU's data protection guidelines. The European Parliament followed its lead in November 2001. But the Council of Ministers backed away from this full "opt-in" policy in December, and amended it so that sites would only have to notify users that they were placing cookies on their hard drives. The new version of the policy will need to be approved by the European Parliament, before individual states ratify it into their own laws.