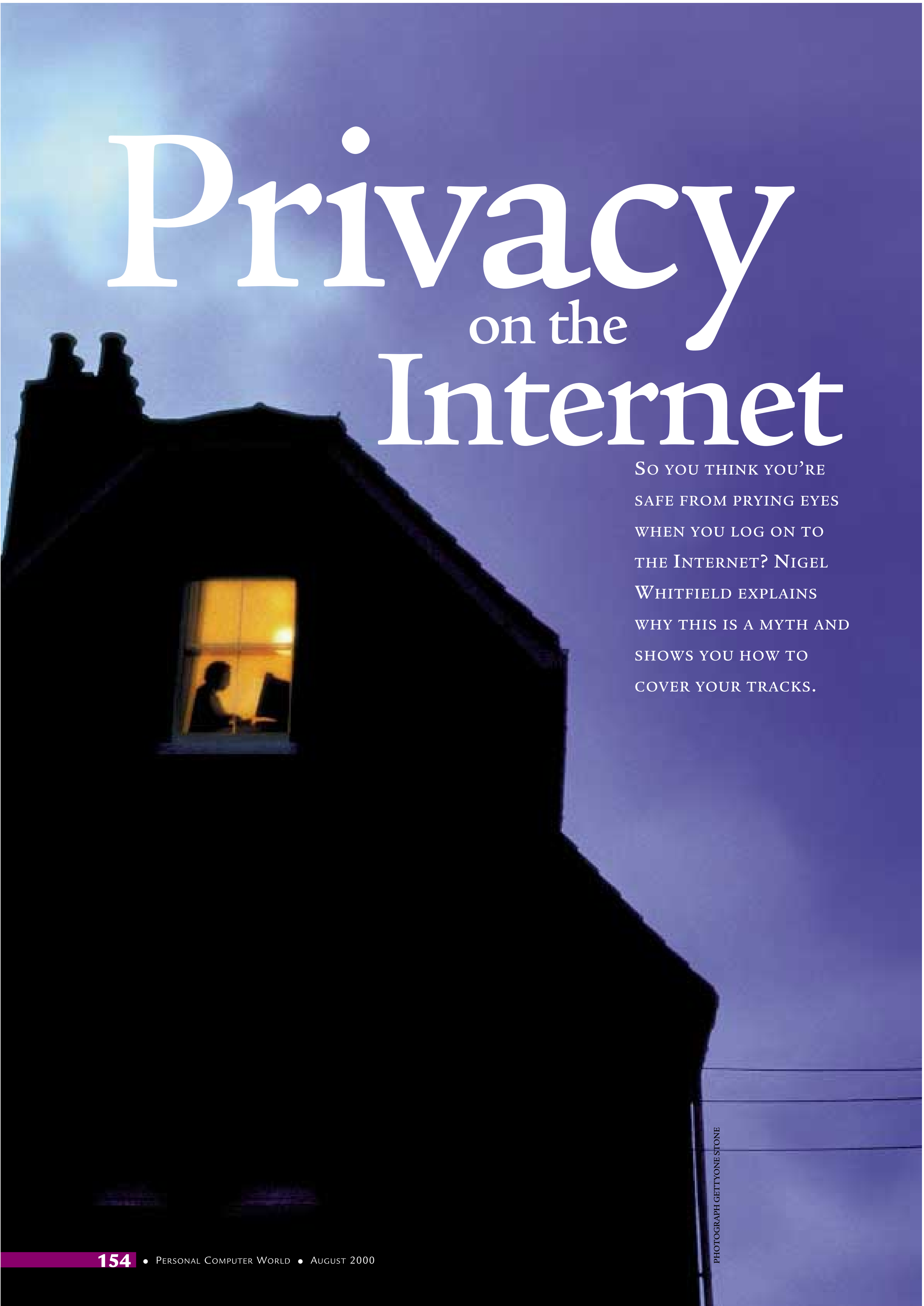


Privacy on the Internet

So you think you're safe from prying eyes when you log on to the Internet? Nigel Whitfield explains why this is a myth and shows you how to cover your tracks.

PHOTOGRAPH GETTYONE STONE

There's a widely held belief that the Internet is anonymous. Most people think they can visit websites around the world, safe in the knowledge that no-one can track what they're doing. They think they can join discussion groups and talk about personal issues, such as alcoholism, worries that their partner is having an affair, or dealing with sexual problems, and no-one will know their identity.

People assume that doing all these things – and more – is safe and private, beyond the reach of anyone who wants to find out what's been going on.

But it's all a myth. The Internet may appear anonymous when you can wander into a chat room using a made-up name, and say something as outrageous as you like but, as in Hansel and Gretel, there's a trail of bits left behind you.

If you're concerned about your privacy there are a couple of questions to ask: how visible is your trail, and how hard will it be to follow?

Privacy on the net is an emotive subject, but it's best approached rationally. There is, for instance, little point becoming stressed over an ad agency tracking which of their clients' sites you visit online when you freely hand over a loyalty card in the supermarket each week.

Watch it!

Before you can understand how to protect your privacy, it's helpful to know just what information you're generating when you connect to the net, and how easy this is to trace.

At the very lowest level, when you connect to a site on the Internet, that site will receive a record of your IP address – the unique number that indicates which computer you're using. If you use an ISP like Demon that gives you a fixed address, that's enough to pinpoint your account. With a dynamic address, it'll pinpoint instead the modem line you connected to. Finding out which customer was using that line means matching up a time with the logs from the computers that handle your login. On a busy system that could mean finding one from tens of thousands of entries, but it can be done. This is how the police were able to track the source of the Love Bug virus to a dialup account used by a group of students in the Philippines.

Some systems, such as AOL, might share an IP

Is it a case of RIP privacy?

A hot topic for anyone concerned with privacy on the net is the Regulation of Investigatory Powers (RIP) Bill, presently going through Parliament. It should be on the statute books by October; in fact, it needs to be, otherwise interception of some types of communication will fall foul of the Human Rights Act.

The official line on the Act is that it simply updates the law to provide for interception of electronic communication along the same lines as presently allowed for phones and the post – subject to the issuing of a warrant.

However, there are areas that cause considerable concern to many people. One of the most controversial is the requirement that ISPs provide a means for interception, essentially building into the UK Internet infrastructure an organised system for monitoring. While the Government may pay the costs of setting the system up, it's likely that ISPs will have to pay annual fees, which in the case of the largest could amount to hundreds of thousands of pounds. Given that ISPs are not the most profitable of businesses, many may find that too onerous a burden, despite the contrary claims of a Home Office report.

When the system is in place, an ISP may be notified that an interception is required based on the email address, home address, or postcode of a target. The Bill also provides for interception of the complete IP datastream for a suspect, as well as just email.

Another area of concern is encryption. While the Government has abandoned any plans for a key escrow system – where a 'trusted' party has to hold copies of keys, and will produce them on demand – the provisions in the Bill have worried many people, not least because they appear to reverse the traditional burden of proof in a court.

When encrypted information needs to be decrypted in the course of an enquiry, you will be required to hand over the keys to unlock that data. If you don't comply, you could face up to two years in prison. If you don't have, or never have had, the keys or you have forgotten your password, you have to prove that's the case, or face the consequences. In other words, guilty until proven otherwise. Whether this system will survive the test of the Human Rights Act remains to be seen.

The penalty may even be increased on the grounds that criminals may refuse to hand over keys to data and suffer two years in prison, rather than the longer sentence that might result if incriminating data was exposed.

For more visit www.stand.org.uk.

address between more than one user; the same is true of some corporate gateways to the net, but even so, there will usually be a way to work back to a specific system, even if it involves trawling through pages of log files.

Recording which IP address accessed a site is a start, but it's not enough for many places on the net. They want to know more, like if you've visited before, for instance.

That's done using cookies. There are many myths about cookies, best dispelled by looking at a site such as www.cookiecentral.com. A cookie is simply a piece of information that a website asks your browser to store on your PC. The same site can then request the cookie next time you visit. That allows it, for instance, to automatically fill in your login name on the AvantGo pages, or supply the weather reports you asked for on the MSN.co.uk home page.

What a cookie can't do is trawl your hard drive for your credit card number. It can't tell a website anything it didn't already know about you – and if you tell a site your name is really Cecilia instead of Charles, then that's what will be in the cookie that's stored on your computer.

So why do so many people get worked up about cookies? Simple. Because a few companies, most notably DoubleClick, have found a way round the fact that a server can only request cookies for its own site.

DoubleClick is an ad agency that supplies the ads that appear on many of the net's most popular sites. Using cookies, DoubleClick can uniquely identify you, building up a profile of what type of sites you visit, and displaying appropriate adverts.

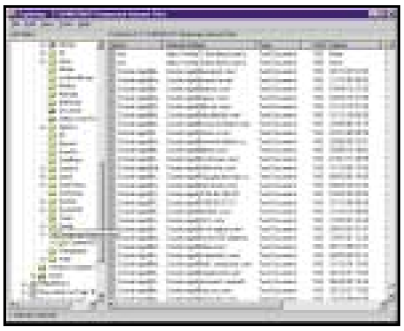
How can it do that when cookies are unique to a site? It's simple – the DoubleClick adverts aren't on the site you visit. They're stored on DoubleClick's own servers, and your web browser dutifully fetches them from there. That means it's requested information from the DoubleClick server, and so it can have a cookie sent, or passed back to, that server. The link to ad will indicate which client site it's come from, allowing a profile of the type of sites you visit to be built up, even supplying relevant adverts for you.

I am not a number

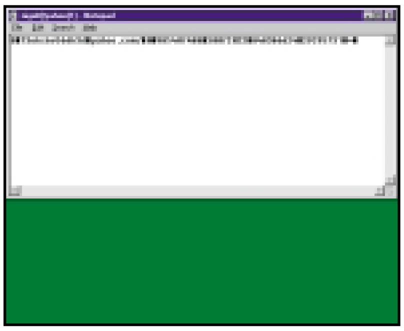
As long as none of the sites that you visit requires you to register, you're just a number – a unique ID that lets people analyse trends, but keeps your true identity private.

Register for a site, however, and information

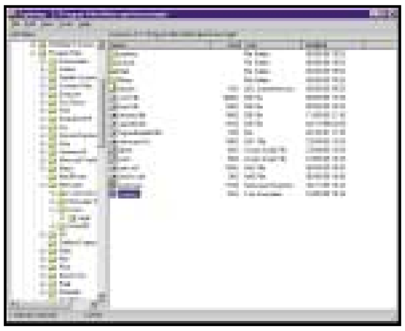
How to find cookies on your system



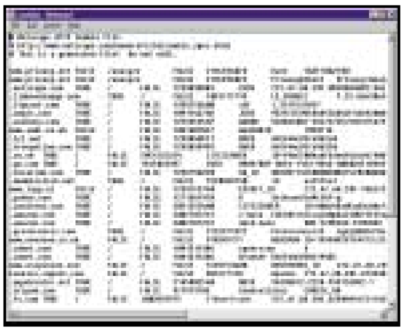
Purging your browser's history isn't enough to cover your tracks. Many sites leave a cookie on your computer, which will last far longer than any history list. Open your Windows\Temporary Internet Files folder, and you'll see a list showing plenty of items from sites you've visited; sort by Type, and all the cookies will be grouped together, as shown above. On systems where you use a login name, each cookie will begin with the name of the user who owns it.



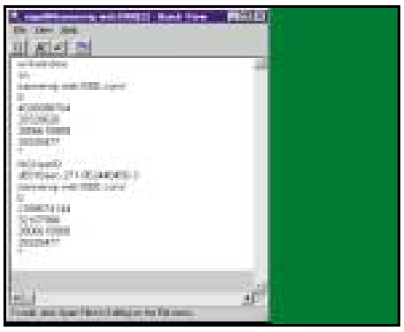
1 Each cookie is just a text file; double-click to open it and you'll see the information that it contains. In many cases, such as the one above, it'll just contain a random ID number for a particular site, along with the expiry date and the domain it belongs to. Some cookie files, however, may contain a user name that you use on that site.



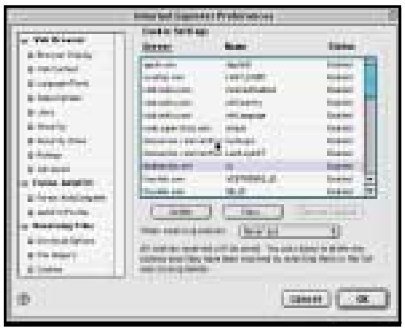
2 Older versions of Internet Explorer stored cookies in \Windows\Cookies, so check in there to see what other cookies lurk on your system. Netscape stores all the cookies in a single file, cookies.txt, which you'll find in the sub-directories of Netscape's users folder, for example, \ProgramFiles\Netscape \Users\nigel\cookies.txt. Mac Netscape users can look at their cookies in the Netscape Users folder within the System:Preferences; the file is called MagicCookie.



3 This is the content of Netscape's cookies.txt file – each line corresponds to a cookie, giving the domain name, the path, whether or not there should be a secure connection, and expiry information, as well as the cookie data itself, in the last column. The first TRUE/FALSE entry specifies whether the cookie can be used by the whole of the domain to which it applies.



4 Microsoft's QuickView is a better bet for opening cookies than Notepad. If they're stored in the Temporary Internet Files folder, then you can see the expiry date and when they were last accessed – the Cookies folder doesn't store that information. Times are stored in the Unix time format – seconds since the start of 1970.



5 Users of Internet Explorer on the Mac have the best solution – from the Cookies option in Preferences, you can see all the cookies on your system, and just a simple click will display them clearly, with all the information formatted correctly. Sadly, you can't edit a single cookie to corrupt its data.

that you supply, such as name and address, age, nationality and so on, may be passed back to the advertising company. In the US, DoubleClick has caused a storm by buying a traditional marketing agency, stoking fears that comprehensive online and offline profiles about people could be built up.

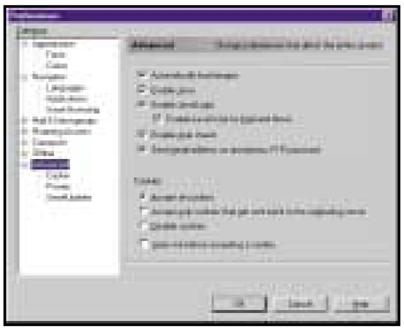
If you're using a fixed net link, it doesn't even take registration to glean at least a little more information about you. Commonly available tools can turn an IP address into a real street address – or at least the address of a person who registered a particular domain, or had a certain range of addresses assigned to them. So, for example the IP address 212.161.108.129 can be traced to 32-34 Broadwick Street, London W1 – the home of *PCW*'s publishers, VNU.

One way of hiding the websites you're visiting is to go via a proxy, then the address that appears in the web server's logs is that of the proxy server. Of course, all that's really doing is adding another link to the chain, since the

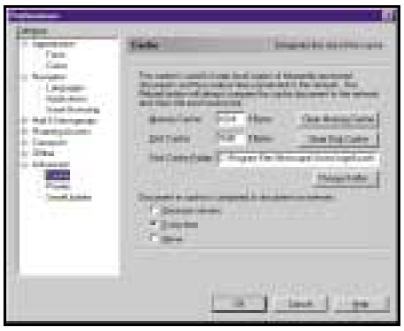
QUICK TIP

Editing the cookies for ad services by changing random parts of the information will ensure that they find it hard to track you accurately. You can also mark the cookie as 'read only' in Windows to stop it being updated.

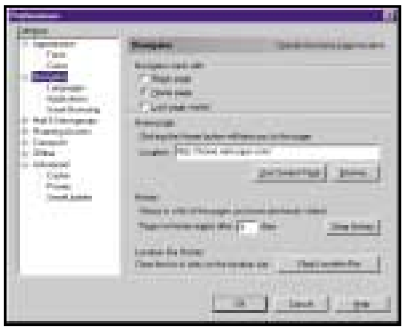
Keeping your web habits private



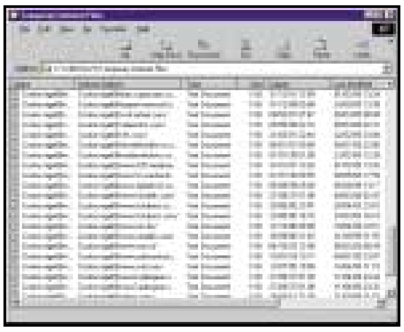
With a little work, it's fairly easy to stop people gathering information about your web habits, both online and if they have access to your PC. Netscape users can tell the browser to ask them before accepting a cookie in the Advanced section of the Preferences window. You can also disable JavaScript on the same screen, which stops sites finding out things such as the resolution of your screen, or the time zone of your PC – but other features will no longer work.



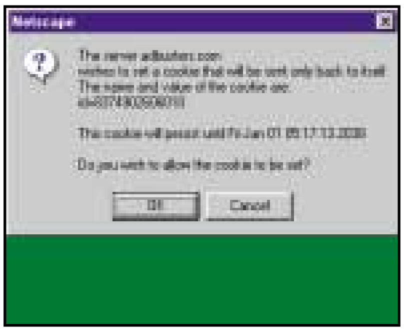
1 Clearing the disk cache makes sure that people won't be able to see what you've been looking at. You can also change which folder information is stored in, so you could cache everything on a removable drive, like a Zip, if you don't mind the resulting slower performance. That way, you'll have the convenience of caching, without exposing your files as much. Changing the path will also fool security exploits that rely on knowing the location of files on your PC.



2 The main Navigator preferences in the browser let you set how many days worth of sites are stored in the history – which is a .dat file in your user preferences folder. Again, you can clear this out to prevent people being able to see where you've been, but you'll need to do more cleaning up after quitting the browser to be really safe from prying eyes.



6 This is what's left in the Temporary Internet Items folder after you've used the Clear button. To get rid of the cookies, you'll have to delete them manually. There may be a few that you want to keep, to save having to type login information for some sites you visit regularly. In that case, delete the others, set the ones that you want to keep to 'read only' to stop them being updated, and tell your browser not to accept any other cookies.



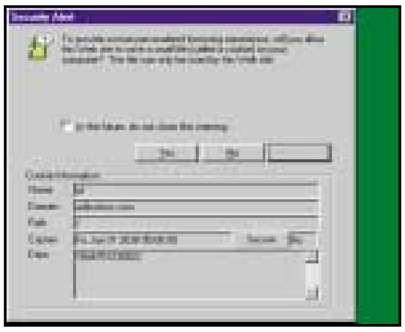
Netscape

The server adbusters.com wishes to set a cookie that will be sent only back to itself. The name and value of the cookie are: id=83774902908018

This cookie will persist until Fri Jan 01 05:17:13 2038

Do you wish to allow the cookie to be set?

7 Netscape users will see this box when they've asked to be warned about cookies. Although the dialog says that it will persist – there's no option in Netscape to automatically reject only persistent cookies – you can stop it persisting by making your cookies.txt file read only, as explained in step three. Click Cancel if you don't want to accept the cookie.



8 Internet Explorer displays a fairly uninformative message when a cookie arrives, if you've asked to be warned. Click on More Info, however, and you'll see a display similar to this one, giving full information about the cookie that's being sent. For sites such as this, a dummy ad network demonstration via www.privacy.net, you could make a note of the ID, then edit it in the cookie file to prevent accurate tracking of your web activities.

QUICK TIP

You can hide the websites you visit by using Anonymizer, at www.anonymizer.com. Type the URL you want to visit into Anonymizer's web page, and you'll see the site over an encrypted connection.

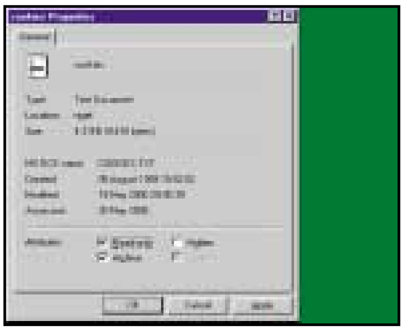
proxy server will have a record of what you're asking it for.

This is also what makes proxy servers a useful tool for those who want to see what you're doing. Even though you may not think your web requests are going via one, many ISPs use 'forced' proxying. That means that all web requests are routed via a transparent proxy. You don't need to change any settings in your browser, but the effect is the same. And for an organisation or country that wants to control and monitor what people are seeing on the web, it's ideal.

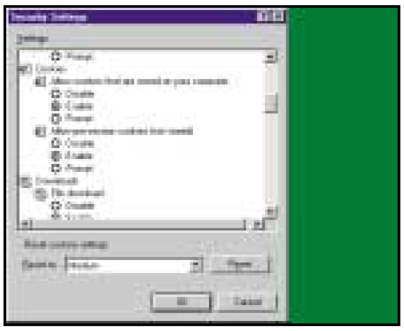
More than the web

There's much more to the Internet than the web, of course. Email is one of the most popular ways of communicating and, once again, everything you do – the sender of each message you receive, or the destination of each message you send via your ISP's mail server – will appear in logs.

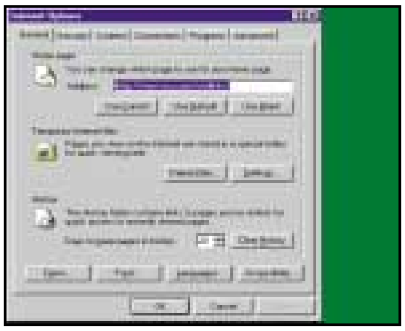
A trivial tweak of an alias file could forward a



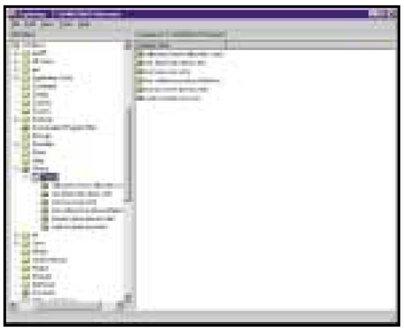
3 If you don't want to be bothered with the prompts each time a cookie arrives, you can instead right-click on the cookies.txt file in your Netscape user preferences folder, and set the Read Only attribute. That has the effect of making cookies 'session only'. They'll work within a browsing session, but they're not saved when you quit the browser. You could also edit the cookies file so that it only holds those for sites where you really do want them saved.



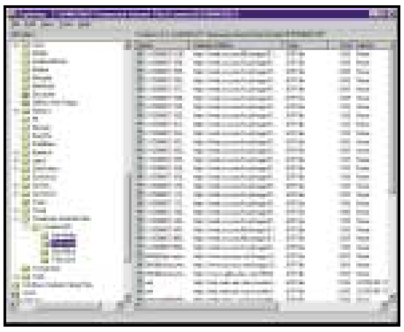
4 In Internet Explorer, choose Internet Options from the Tools Menu, then Security, Internet Zone, and click on Custom. Scroll down to find the options for cookies. IE allows you to set different options for session cookies, and persistent cookies. The same dialog box lets you specify options for scripting and Java.



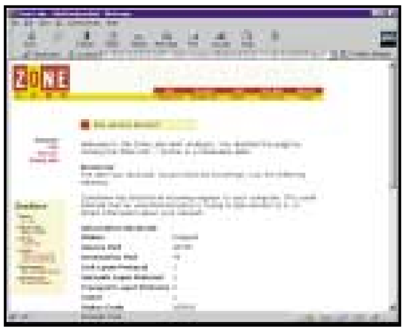
5 The General tab allows you to set how long pages are stored in the history, and the size of the Temporary Internet Items folder. You can empty stored items from that folder using the Clear button, but cookies won't be erased – just images, pages and other items. You'll also have to look elsewhere (see next page) to completely cover your tracks.



9 Even if you clear history and cache files, some traces will still be left behind. After you've quit the browser, you can tidy up the hard drive on your PC. This is the Windows\History folder, which has folders for each site you've visited. You can delete all the files here safely, but remember that to really cover your tracks, you should use a proper file wiping tool, to prevent an undelete program from recovering a list of sites you visited.



10 IE5 could almost have been designed to leave a trail on your hard drive. As well as the Temporary Internet Items folder, you'll find information, including cookies, in sub-directories under the Content.IE5 folder too, so you'll need to erase all those if you want to be sure of stopping people from seeing where you've been browsing. And while some versions of IE used just the Temporary folder, or just the Cookies folder for cookies, IE5 appears to use both!



11 Netscape's cache folder – there's one for each user – is a little harder to interpret, since items in it have random names but, nevertheless, the files in it can still be opened if someone's determined to see what you've been looking at, so once again, it's a prime candidate for completely wiping if you want to maintain your privacy.

copy of all your incoming mail to someone else and it's not much more work to intercept outgoing messages. Following the introduction of the Regulation of Investigatory Powers (RIP) bill later this year, all ISPs will have to provide a means to intercept email when a warrant is issued.

Depending on the type of network used, it may already be easy for other people to read your messages, and in some countries, companies have no qualms about looking at the contents of email that their employees send or receive.

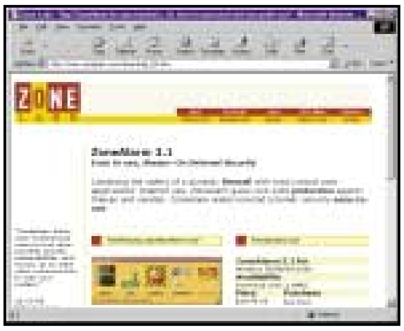
Besides email, just about any other connection-based service on the net can be logged, with a computer somewhere recording the time and source of each connection it receives. And with access to the network your information is passing over, such as via your ISP, it's theoretically possible to monitor each packet of data, examining its source, destination and contents.

Don't forget that your movements can be tracked when you're offline too, by anyone with

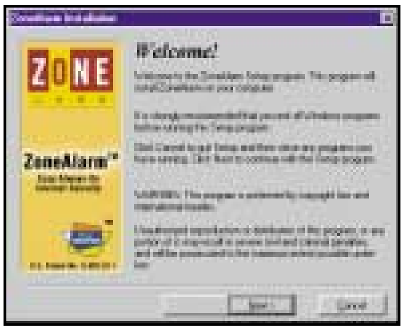
QUICK TIP

If you don't want your email address known, make sure you use a modern web browser – some older ones send your address each time you download a file via FTP.

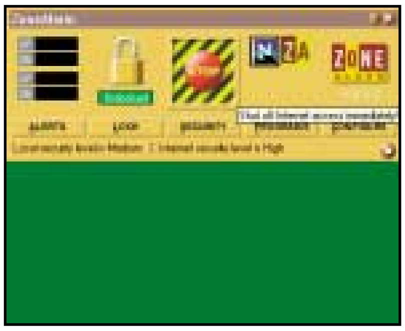
Using Zone Alarm to increase your PC's security



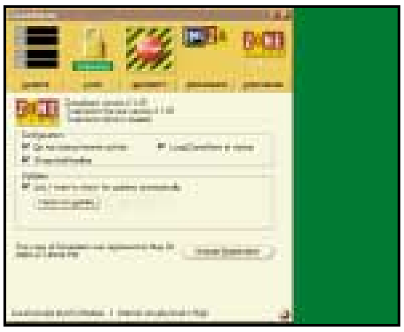
When you connect to the Internet, you're also at risk from malicious programs, received via email, IRC or from websites. Some of those, such as BackOrifice, could give people access to your computer, so a firewall of some sort is essential. ZoneLab's Zone Alarm is free for personal or non-profit use, and can be downloaded from its site at www.zonelabs.com. The latest version will also stop you executing VBS scripts received over the net – such as the Love Letter virus.



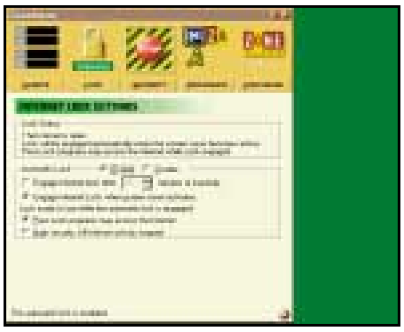
1 After you've downloaded the file from the net, just run it and you'll see a screen similar to this one. Installation is simple, and you'll just have to answer a couple of questions about whether you're using it for personal or business use, and which folder it should be put in. After installation, restart your computer, and Zone Alarm will run automatically, protecting your system right away.



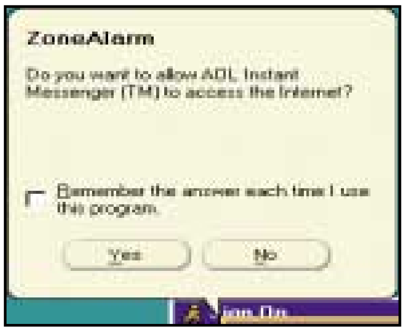
2 This is the main screen; even if you close this window, Zone Alarm will carry on running, and you can relaunch the control centre by double-clicking the icon in the system tray. The bars on the left show net activity, while the Lock and Stop buttons allow you to restrict or halt Internet activity immediately.



6 The Configure button displays this panel, allowing you to turn off the automatic loading of Zone Alarm, and whether or not it's always floating above your Internet apps – which can be a little annoying if you don't have a large monitor. Business users will have to pay for their copy of the program after a trial period; you can change registration details via the button at the bottom of the panel.



7 The Lock screen lets you turn an 'Internet lock' on and off, giving additional protection, for example whenever the screensaver kicks in. That way, you can have greater access when you're using the computer, and you don't have to remember to do anything when you take a break. The 'Pass Lock' option means that some programs can carry on accessing the net, even when others are locked out.



ZoneAlarm

Do you want to allow AOL Instant Messenger (TM) to access the Internet?

□ Remember the answer each time I use this program.

8 While Zone Alarm is running you'll see a warning like this when some net activity is detected – though not necessarily as soon as you start a program. The message appears when the program starts to access the Internet, and you can grant permission each time, or have Zone Alarm remember your decision. The control panel will tell you which programs are accessing the net at any time.

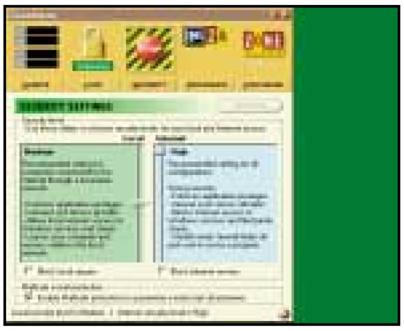
access to your PC. Your web browser will record all the sites that you've visited in its history file, and some pages will be cached. It's not that hard to turn the history and cache files back into a list of sites or pages. People have already fallen foul of the law because of the traces left on their computer after they've visited sites.

Some recent security exploits have showed that it's possible to read a file on a PC if you know the path – something that's dismissed as not too likely by browser writers. But there's a safe bet, for instance, that if you use Netscape and accepted the default options, you'll have a file called C:\Program Files\Netscape\Users\default\netscape.hst, or cookies.txt, either of which could reveal information about your habits if read by someone else.

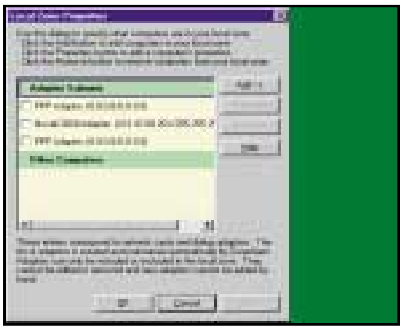
The truly paranoid might decide never to use the Internet, so great are the opportunities for tracking what people do. Or the complacent may fall back on the old adage that the innocent have nothing to fear.

QUICK TIP

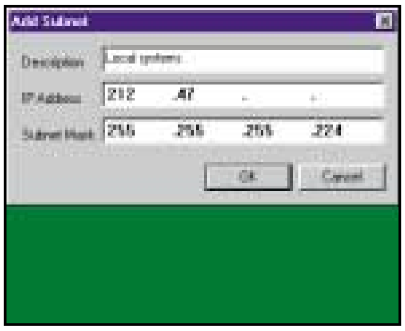
Netscape and Internet Explorer store cookies in different places, so you could configure one to reject cookies for casual browsing, and use the other to visit only 'trusted' sites where you're happy to accept them.



3 To start with, click the Security button to reveal this screen and check that the settings are suitable. If your computer is on a network with others, you'll need to make sure that they can access any resources they need on the protected system. For most users, the default settings will be OK. At the bottom of the screen, you'll see a checkbox for protecting you against script viruses received via email. Unless you have a good reason, ensure that this box is checked.



4 Click the Advanced button, and you'll see this screen, which allows you to specify other computers that you want to include in your 'local' zone, which will allow them a higher level of access to your PC – perhaps being able to share files, for example. Click the Add button to create a new entry.



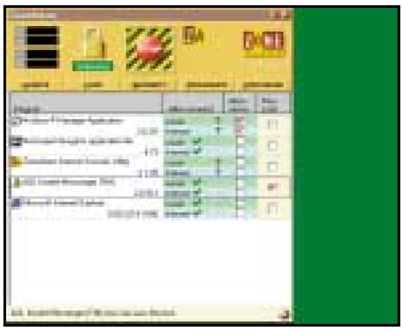
Add Subnet

Description: Local systems

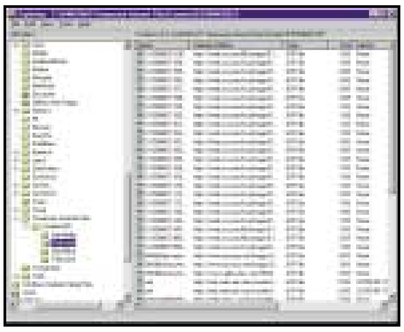
IP Address: 212 . 47 . .

Subnet Mask: 255 . 255 . 255 . 224

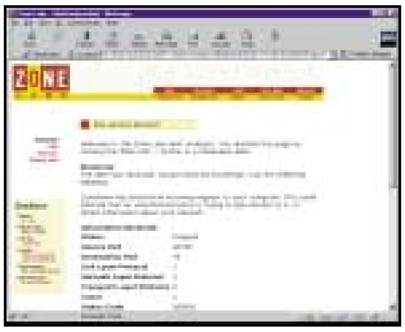
5 Rather than specifying a single machine, you can use a network number and hostmask, as we've done here, to add a whole range of TCP/IP addresses. For most users, this will be a private IP address range. The numbers you enter here should match those that you have configured for the other hosts on your network. Add the new entry, click OK, and then OK again to close the Advanced settings dialog box.



9 The programs panel lets you set options for each of the Internet applications on your system, including whether or not that program can act as a server, receiving incoming connections. IRC, for instance, needs to do that for some functions like DCC to work properly. The Pass Lock column lets you specify if the program can run when the net is otherwise locked, and for each program you can set different options for the local zone and the net.



10 This is the alerts screen, which lets you review all the connection attempts that have been made to your computer, so you can see if someone's been scanning it for Back Orifice, for example. If there's a particular service running on your system, such as Windows File sharing, that someone tries to connect to, you'll also see a warning message when they attempt to connect, and you can allow them if you know who it is.



11 Click on the More Info button when you're viewing an alert, and your web browser will attempt to look up information on the ZoneLabs site, where you'll also find more details about how to set up popular programs to work with the improved security of your system. And that's all there is to it – with just a few clicks, you've dramatically increased the security and privacy of your computer.

As ever, the truth lies somewhere in between. You can take steps to protect yourself, to stop the marketing companies making your life into a data set for their analysis by managing cookies properly. And you can prevent your partner knowing what websites you've visited using a service like anonymizer.com.

But while you can take comfort in knowing that the sheer volume of information generated across thousands of computers by the millions of net users makes it hard to single out one person for attention, rest assured that if an official agency really wants to know what you're up to, it can make a pretty good stab at finding out.

Privacy on the net isn't a complete myth, and the casual user can follow some of our simple steps in the walkthroughs above and on the previous pages to increase it. Ultimately, privacy or the lack of it are very similar online – both can be arranged, but you need to be pretty determined to achieve either.

QUICK TIP

Discover what tricks and tips are used to find out about you by visiting www.privacy.net, and asking for an analysis of your connection.