

Stop Big Brothers!

SUPREET SETHI

The Internet is a great leveller. Everyone can use it to get and exchange information efficiently. Some of us are servers and producers of this information, but most of us merely use it. Obviously, one can find out information about those who serve the material, but interestingly enough, none of us are exempt from this watching eye. There are many ways to get information about a person on the Internet as somewhere, somehow, there will be record about where you have been. And anyone can pick this up.

Lets take an example. Point your browser to any search engine and search for <your name>, or my name. If you have been actively participating in any Internet based activities like a mailing list, your name would definitely pop-up in the search. This may seem like redundant information collected and archived by a search engine, but there are many companies that actively acquire and analyse such information for their benefit.

This practice - known as profiling - is used for co-relating online activities with activities in the physical world, and it is used for targeting advertisements accordingly. Companies make huge profits by selling this data to others. One such company is Doubleclick Inc., the largest ad site. About 11,500 sites carry the DoubleClicks banner ad.

Many and Different Ways

There are various other ways to get info about you if somebody wants to. I have to get only one e-mail to tell me what kind of operating system you are using, from which network or ISP you are coming from, and so on. All this is available in the header that is attached to every e-mail. For example:

```
[Received: from ludworth.uklinux.net (chris@ppp-1-19.cvx2.telinco.net [212.1.140.19])
X-Mailer: Mozilla 4.06 [en] (X11; I; Linux 2.2.16 i586)]
```

Consider the above text. It is appended to the mailer when the mail was transferred to reach me. What I can infer from this is:

1. When the person mailed me his/her IP address was 212.1.140.19 and he/she was using the dialup facility to connect to Internet.
2. Lives maybe in the UK, and using this IP address I can trace the person all the way to the ISP. If I put in some effort I can even get to know the city he/she lives in.
3. He/She uses Netscape on the Linux platform in a Pentium class machine

A similar text gets attached to any website request your browser makes. These are sample log files of my web server.

```
127.0.0.1 - - [01/Jan/2001:04:34:16 +0000] "GET/images/book.gif HTTP/1.0" 200
964 "http://127.0.0.1/images/" "Lynx/2.8.3rel.1 libwww-FM/2.14"
```

This information in itself does not speak much but it all has more meaning when

cookies are sent to you and your browser accepts it. This is the kind of material that Doubleclick would be looking at.

So whether it is business transactions or a private affair, information can be gathered and used against you for others' personal benefit or for causing some harm to you.

The question that remains mostly unanswered is, "What can be done to 'anonymize' your identity?"

A few simple steps that can get you out of the public eye to a large extent:

1. You should use an anonymous proxy for surfing websites. Web sites are requested for by the browser. If a proxy is being used, the request is transferred to the proxy software and it handles the request and then sends back to you the pages and their content. Anonymous proxies do not reveal your identity when you make a request. Another interesting benefit of using proxy is that the local ISP cannot stop you from surfing certain sites because you are not directly requesting for any sites.

2. Using the anonymous remailer service which is provided by many sites. You mail them your mail, and they will redirect it to the concerned person or group.

3. PGP (Pretty Good Privacy) can be used to encrypt your mails, allowing only the concerned person access to the mail in clean text, even if the mail is snooped. For PGP, the person the email is being sent to releases his/her public key. When you want to send a mail to that person you use his/her public key to encrypt the mail. Then he/she would be able to decrypt and read the mail.

Sites worth visiting in this context are:

www.privacy.net

www.privacytimes.com

www.anonymize.net

Privacy is not about sending a few mails by remailer, surfing certain sites with third party proxy or using PGP for a particular message. It is about using such services on a regular basis. Remember, there is security in numbers.

