Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:4A
Received 6 August 2003

Ms Irene Graham
Executive Director
Electronic Frontiers Australia Inc.
PO Box 382
NORTH ADELAIDE SA 5006
☎07 3424 0201 07 3424 0241
E-mail: ed@efa.org.au

Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 07 3424 0201
Fax: 07 3424 0241

6 August 2003

The Committee Secretary
Parliamentary Joint Committee
on the Australian Crime Commission
Suite S1 107
Parliament House
CANBERRA ACT 2600

Email: acc.committee@aph.gov.au

Dear Ms Weeks

Subject: Inquiry into recent trends in practices and methods of cybercrime

EFA has reviewed the transcripts of the Committee's hearings held in mid July and we wish to offer the Committee further information in relation to some of the matters discussed and proposals put forward. To that end, we attach a supplementary submission.

We recognise that Committees are not required to accept supplementary submissions and whether or not the Joint Committee wishes to do so in this instance, we hope the information will be of assistance to Committee members during the course of the inquiry. (Also, please be aware that although we refer to the attached as a submission, we are not seeking to attract parliamentary privilege in relation to the content − there is no information in the attached that needs such protection.)

We would be pleased to respond to any questions that may arise from the attached information.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Supplementary Submission to the Parliamentary Joint Committee on the Australian Crime Commission

Inquiry into recent trends in practices and methods of cybercrime

6 August 2003

Contents:

Introduction

Further to EFA's submission dated April 2003 and testimony before the Committee on 21 July 2003, we have reviewed the transcripts of the Committee's hearings on 17, 18 and 21 July 2003.

In this submission we address proposals put forward during the hearings for prohibiting free email accounts and requiring 100 point ID checks. We consider these ideas would be largely ineffective and quite probably counter−productive, due to the technological and global nature of the Internet.

We hope the below information will be of assistance to the Committee in considering the merits or otherwise of the proposals.

▲ Go to Contents List

France − 100 point ID *not* required for Internet access

We note the remarks made by a witness during the hearing on 21 July 2003:

> "...In 1996 I suggested that everybody who used an Internet account should have to go through a 100−point check, the same as if opening a bank account. ... France, as far as we are aware, is the only country that has done anything about it. About two years ago it enacted such provisions. ..."
> ...
> "Mr SERCOMBE—Could you give us some further information about the experience in France?"
>
> "... I left the the NCA at the beginning of 2000. ... As to what has happened, I am afraid I cannot take it any further. ..."

We advise that such a requirement has not been enacted in France, nor was such a requirement introduced into the French Parliament in 1999/2000 (nor since then).

In 2000, the French Parliament reviewed the *Liberty of Communication Act* (*Loi sur la liberté de communication*) which generally addressed audiovisual broadcasting communications. Several new provisions regarding Internet service provider liability were introduced which attracted widespread criticism. One of the amendments concerned identification. However, it was and is only applicable to web site content providers, not persons who wish to open an Internet access account or email account (free or otherwise).

As stated in *Privacy and Human Rights 2002*, an annual international survey prepared by the Privacy International and the Electronic Privacy Information Center, issued in September 2002:

> "The French Liberty of Communication Act was adopted on June 28th, 2000. The Act requires all persons wishing to post content on the Internet to identify themselves, either to the public, by publishing their name and address on their website (in the case of a business) or to their host [ISP] provider (in the case of a private individual). Earlier provisions, which would have imposed large penalties and jail sentences on anybody violating this requirement and required Internet Service Providers (ISPs) to check the accuracy of the personal details given to them, were dropped in the final version of the legislation."
>
> (*Privacy and Human Rights*, Part 2 − Country Reports: Argentina to Lithuania http://www.privacyinternational.org/survey/phr2002/phr2002−part2.pdf 985 Kb)

A full history of the developments since the law was first proposed in May 1999 is available (in French) on the website of IRIS, a French civil liberties group, at: http://www.iris.sgdg.org/actions/loi−comm/index.html

At the time the above law was under consideration by the French Parliament some people distributed misinformation on the Internet stating that identification requirements would apply to "activities such as participation in chat rooms, online message boards, mailing lists, etc". Such claims were not correct. The identification component of the law applies only to web site content providers and ISPs are not required to check that their personal details are accurate.

▲ Go to Contents List

Free email accounts

We also note remarks suggesting that prohibiting free email accounts would make life easier for law enforcement agencies.

> "A short−term fix which would make life a lot easier would be to do away with free Internet accounts such as AOL and Hotmail and matters such as that, because if Internet accounts are not free, people have to pay by credit card, and the vast majority of people who use credit cards have provided appropriate information when obtaining the credit cards and that gives law enforcement some starting point. I am aware, of course, that any serious criminal is going to have access to false credit cards or credit cards with false details, but at least it is a start."

We wish to draw to the Committee's attention that doing away with free email accounts, even if that was globally feasible, would not make any difference to the ability of LEAs to identify the user of the free email account.

The issue for LEAs is not whether an email account is free, it is whether the sender of an email can be identified.

There is a widely held mis−perception that users of free email accounts such as those provided by Hotmail are anonymous. This is not necessarily so. In the case of Hotmail for example, the sender's IP address is included in the header fields of the email message and can be used to identify the owner of the Internet access account being used at the time the message was sent.

An individual may have an Internet access account provided by an Australian ISP and be connected to the Internet using that account. The individual may also have a free email account provided by Hotmail in another country. When the individual sends an email message using their Hotmail account, the header fields will show, for example:

> Received: from 203.143.248.163 by by2fd.bay2.hotmail.com with HTTP; Mon, 12 May 2003 08:30:57 GMT
> X−Originating−IP: [203.143.248.163]
> X−Originating−Email: [anon1@hotmail.com]
> From: "anon1" <anon1@hotmail.com>
> To: ...@...
> Date: Mon, 12 May 2003 08:30:57 +0000
> ...
> Message−ID: <bay2−F32J8w8wPzJ0851000642c@hotmail.com>

Whether or not Hotmail knows the real name and address of the user "anon1", LEAs can and do use the originating IP address [e.g. 203.143.248.163] to find the sender. The LEAs can look up the IP address (there are many free IP address lookup services on the Internet) to find out which ISP owns that IP address. The LEA then asks that ISP which one of their customer Internet access accounts was connected to that IP address at the time the email was sent via the Hotmail service. Information about the means by which an ISP can identify the customer account is provided later herein.

The IP address is a more reliable means of locating the sender than identifying the owner of the Hotmail account "anon1@hotmail.com". An email address is a very weak identifier because it is trivially easy using many email software products to falsify the email address in the 'from' field before sending a message. A criminal could put someone else's email address in the 'from' field.

(There are also numerous law−abiding reasons to use a different address in the 'from' field. For example, a person sending a work−related email from home may use their work email address in the 'from' field of that message, and use their personal email address in the 'from' field when sending a personal email.)

Although many email services place originating IP addresses in the header fields of an email message, individuals may also use a free or commercially provided anonymising service which strips the originating IP address from email messages. See later herein.

▲ Go to Contents List

Chat Rooms

Many chat room facilities are provided by organisations and individuals around the world who do not provide Internet access accounts. Some of these providers log the IP addresses of users of their chat room and some do not. If the IP address is logged and if the chat room provider provides the IP address to an LEA, then the LEA can contact the ISP who owns that IP address to find out which of the ISP's customer accounts was using that IP address.

Although a chat room may log IP addresses, individuals may access a chat room via a free or commercially provided anonymising service which discloses to the chat room only the anonymising service's IP address, not the user's IP address. See later herein.

▲ Go to Contents List

How an ISP identifies which customer is or was using the Internet and can monitor/track activities

All computers connected to the Internet have an IP address, e.g. 203.143.248.163. The IP address is used to direct traffic over the Internet. For example, when a user clicks on a web page address, the web server checks which IP address requested the web page and sends the content of the page to that IP address and it is then displayed on the user's computer screen.

An Internet user can find out which IP address is being used to direct information to their computer by using, for example, a service such as those available at:
http://snoop.cdt.org/snoop_on_me.shtml
http://privacy.net/analyze/

The ISP who provides a person with Internet access allocates an IP address to the user's computer when the person connects to the Internet.

For example, in the case of a dial−up user, when the person dials into an ISP's log−in system, they enter their username (e.g. "jsmith") and password. This information is passed to the ISP's RADIUS server (Remote Access Dial−In User Service). Detailed information about RADIUS servers is available in many documents online, e.g.:
http://rfc.net/rfc2138.html
http://www.telstra.com.au/dialip/docs/radius.pdf

The RADIUS server checks that the username and password are valid for access via the ISP's system and, if so, authorises log in to the Internet and allocates an IP address to the user's computer.

The RADIUS server also logs information about each user's access for accounting/billing purposes. It creates a start record when the user logs in and a stop record when the user logs out. The start record includes, among other things, the following information:

```
Attribute         Example Value           Explanation

Time              Tues Nov 1 9:30:11 2002 Time user connected to Internet
User−Name         "jsmith"                User name logged in with
IP−Address         203.143.248.163        IP Address allocated to user
```

The IP address allocated to the user's computer is the data that can be used to track/monitor a user's activities while connected to the Internet. Most ISPs' systems usually allocate IP addresses to users

dynamically, that is, each time a particular user logs in they are given a different IP address. (This is because otherwise the ISP would have to own one IP address for each customer, although not all customers are always connected.) However, an ISP can configure their system so each time "jsmith" logs in, the same IP address will be allocated.

When a LEA asks an ISP which customer account was used to send, for example, an email message from a Hotmail account using a particular IP address at a particular time, the ISP can check their RADIUS records to find out which customer account was using the originating IP address shown in the header fields of the email message.

Similarly, when an LEA wants to know what Jane Smith was doing or reading during a period of time, the ISP who provides Jane Smith with Internet access can:

- check their customer records to find out Jane Smith's login name, e.g. "jsmith"
- check the RADIUS records to find out what IP address was allocated to "jsmith"
- search for instances of the IP address in their Web server and other logs, e.g. Internet Relay Chat (IRC), FTP, Telnet, etc.

  An example of a Web server log entry (from EFA's web site, with IP address and time altered) is:

  > 203.143.248.163 − − [20/May/2001:09:59:38 +0800] "GET /Issues/Privacy/Welcome.html HTTP/1.0" 200 85 "http://www.looksmart.com.au/r?key=internet+privacy+−+australia3Bus302562" "Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)"

  The above says that at 9.59 am on 20/5/2001 the user on IP address 203.143.248.163 was looking at the page http://www.efa.org.au/Issues/Privacy/Welcome.html and they'd arrived there by searching for "internet privacy australia" using the looksmart search engine.

Searching through all the relevant logs to find out what a user was doing can be time consuming, particularly when the IP address allocated to a user changes each time they log in. However, there are software tools designed for the purpose of automatically searching through and extracting particular information from logs.

When an ISP particularly wants to track and record the online activities of a specific user, they allocate a specific IP address to that user for a period of hours/days/weeks. Then, each time a person logs in with the username "jsmith" everything the user does online will be recorded with the same IP address. This makes it easier to extract the activity data from the logs. ISPs do this, for example, when a law enforcement agency requests an ISP to monitor and record a particular user's activities over a period of time into the future.

▲ Go to Contents List

100 point ID checks for Internet access

We note the interest in ID checks expressed by one Committee member:

> "I find your idea of the 100−point check for service providers interesting. It ties in with the weakness we see at the moment, which is just free access."

Requiring Internet users to undergo a 100 point ID check in order to obtain an Internet access account would have little if any impact on the difficulties experienced by LEAs in attempting to identify serious criminals who use the Internet.

The outcome would be that criminals could have more privacy than law−abiding Internet users. Criminals would use false identity documents to obtain Internet access accounts. Alternatively, they may identify themselves to the ISP to gain Internet access, and then use free or commercially available anonymising services which make it extremely difficult, in some instances impossible, to trace their activities back to the ISP who provides their Internet access account.

Examples of types of anonymising services are provided below.

▲ Go to Contents List

Anonymising Services

Anonymous Remailers

As discussed above many well known free email account services do not provide anonymity.

However, free anonymous remailer services have long been available on the Internet and may be used by whistle blowers and others who have a legitimate reason for sending email anonymously. They can also be used by criminals.

These services strip all identifying information such as originating email and IP addresses out of the email message, before sending the message. Some also send the message through a chain of remailers, none of which know the origin of the message. Some provide an encryption service enabling the sender to encrypt the message which then travels in encrypted format and is decrypted by the last remailer before delivery to the recipient. Serious criminals are more likely to use such services than free Hotmail accounts.

For further information and lists of remailers, see for example:

- Anonymous Remailer FAQ, by André Bacard, Author of Computer Privacy Handbook, [Updated 15 December 2002]
  http://www.andrebacard.com/remail.html
- http://privacy.net/remailer/
- http://anon.efga.org/Remailers/
- https://www.cypherpunks.to/remailers/

Free and Commercial Anonymiser Services

A number of organisations and individuals around the world provide anonymiser services either free of charge or for a fee. There are a variety of different types of services.

Some provide free anonymous web browsing which enables a user to access web sites (including web chat rooms) without their computer's IP address being disclosed to the web site provider. The web site provider receives only the IP address of the anonymiser service.

Others provide a wider range of services for a small fee, e.g. USD$4 per month, long term use for a once only payment of USD$15, etc. Providers of such services offer Internet users anywhere in the world the ability to browse the Web, participate in chat rooms and send email anonymously, that is,

without revealing their IP address. In addition, such services state they do not log IP addresses or retain any other identifying details about their customers or their use of the anonymiser services. The use of such services would prevent an LEA being able to trace an Internet user (who for example sent an email through that service) back to the Australian ISP who provided the Internet user with an Internet access account.

Lists of anonymising services are available, for example, at:

- http://privacy.net/proxy/
- http://www.epic.org/privacy/tools.html
- http://www.samair.ru/proxy/fresh−proxy−list.htm

▲ Go to Contents List

Conclusion

As one witness remarked to the Committee:

> "Every time you lift up a stone, there is something else underneath it. But, although it is an extremely difficult problem, that does not mean that we should not try to tackle it."

EFA believes that tackling the problem of criminals using the Internet by way of prohibiting free email accounts and/or requiring identification checks to obtain an Internet access account are likely to be counter−productive.

The probable effect would be increased awareness and use, by individuals concerned about their privacy, of the methods of protecting privacy and hiding identity online. Use of strong anonymising services by both law−abiding individuals and also those with criminal intent would make it more difficult (and sometimes impossible) for LEAs to track down criminals than it is when individuals use weak anonymity services such as those provided by Hotmail.

Threats to law−abiding users' privacy also tend to result in counter−measures that increase the number and range of privacy and anonymity services available. For example, as stated on the Tonga Anonymous Remailer web site (https://www.cypherpunks.to/remailers/):

> "On September 13, 2001, Lance Cottrell of Anonymizer.com posted the following to the Cypherpunks mailing list.:
>
> > 'In addition to showing that we will not be cowed into giving up our cherished freedoms by terrorists, this is a time when the world needs these services more than ever. In crises there is a tendency for repressive governments to crack down on communications and free access to information. It is at exactly those times that the privacy community must shine its brightest.'
>
> Two days later, on September 15, 2001, the Tonga Remailer was opened."

▲ Go to Contents List