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

12 July 2004

The Acting Secretary
Senate Legal and Constitutional Committee
Room S1.61, Parliament House
Canberra ACT 2600

Email: legcon.sen@aph.gov.au

Dear Mr Bailey

Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Please find attached response to Question on Notice in relation to the above inquiry.

Yours sincerely

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Response to Question on Notice

re: Inquiry into the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*

12 July 2004

Question 1 (Ms Graham, p.5−6, Proof Hansard)

> **Ms Graham**− ... Even if one says that perhaps in some circumstances ASIC should be able to do this or that, this bill is not just dealing with ASIC's perceived problems; it is granting a vast number of agencies increased powers. I would also like to mention that I understand that ASIC probably will not be happy with its powers until ISPs are required to log and record every single thing that an Internet user does on line.
> **Senator LUDWIG**−I do not think their submission goes that far.
> **Ms Graham**−Not in this instance, Senator. But, with respect, submissions by ASIC and AUSTRAC to the former Parliamentary Joint Committee on the National Crime Authority in 2001 did call for powers whereby either ASIC or AUSTRAC−this was reported in the committee's report as well as in Hansard−
> **Senator LUDWIG**−I suppose it is important for ASIC to know which one, though.
> **Ms Graham**−It probably is, but they are all part of the AGEC group.
> **Senator LUDWIG**−I know that, but perhaps you could qualify an agency rather than choose one that might be not the one.
> **Ms Graham**−Yes, I can let you know.
> **Senator LUDWIG**−I am happy for you to take it on notice and let us know.
> **Ms Graham**−I could certainly let you know.

In relation to the above, I now provide the following information regarding ASIC and AUSTRAC.

ASIC has been calling for ISPs to be required to log and retain records of Internet users' online activities since at least 2001. ASIC's statements and activities towards this objective are clearly undertaken on ASIC's own behalf.

With regard to AUSTRAC, it is not clear to EFA whether AUSTRAC's statements and activities concerning ISP logging and record retention are undertaken by AUSTRAC partially on its own behalf, or solely in AUSTRAC's capacity as Chair of the Action Group into the Law Enforcement Implications of Electronic Commerce ("AGEC") on behalf of ASIC and/or other members of AGEC.

More detailed information is provided below.

ASIC

Since at least 2001, ASIC has been seeking laws to compel ISPs to log everything an Internet user does online and to retain logs just in case at some time in the future ASIC or another agency wants to access information in the logs.

According to statements made by ASIC representatives in recent years, ASIC advocates compelling ISPs to record and maintain logs of Internet users' activities due to ASIC's concerns about "false and misleading bulletin board postings in relation to securities on the Internet and the use of spam emails to affect market manipulations and pyramid schemes" and use of the Internet to "promote unlicensed financial advice and to provide hot tips" [1].

ASIC's submissions to the 2000−2001 Inquiry into the Law Enforcement Implications of New Technology, conducted by the Parliamentary Joint Committee on The National Crime Authority ("PJCNCA"), advocated that:

a. ISPs be compelled to log and retain records of Internet users' activities, for example, to log "the details of communications that have taken place and the parties to the communications" and records of web pages accessed (e.g. proxy server logs) [2];
b. ISPs be compelled to monitor Internet users' online activities [2];
c. ASIC be empowered to, by written notice, compel ISPs to immediately stop providing services to an Internet user [3];
d. ASIC be empowered to compel ISPs to remove information from web sites etc [3];
e. ASIC be empowered to make mirror images of hard drives of computers during the execution of search warrants [3].

The Committee's August 2001 Report states that ASIC's submission foreshadowed that the *Financial Services Reform Bill* would give ASIC new powers regarding items (a), (c) and (e) above. However, the Report also states (in Footnote 48) that "The *Financial Services Reform Bill 2001* was introduced into the House of Representatives on 5 April 2001. The issues foreshadowed in ASIC's submission were not included in the Bill" [4].

The Committee did not recommend that ISPs be compelled to do any of the above things, nor that ASIC, or any other agency, be granted any of the above powers.

We note in passing that the Committee's Report states, on the matter of access to the **content** of communications, that:

> "1.67 AGEC subsequently submitted a clear statement of the position taken by law enforcement... In summary, AGEC stressed that there was no question of seeking records regarding the content of communications, since this was already covered by the provisions of the TI Act." [4]

Since 2001, ASIC has continued to advocate that ISPs be required to log and maintain records of Internet users' activities. For example, ASIC's written and oral submissions to the 2003 Inquiry into Recent Trends in Practices and Methods of Cybercrime, conducted by the Parliamentary Joint Committee on the Australian Crime Commission ("PJCACC"), address ASIC's desire that ISPs and other businesses record and retain logs of Internet users' activities because "From time to time ASIC will become aware of postings on a web site that appear to contravene the law. For instance, a series of false and misleading statements intended to induce people to buy particular stock (usually because the offender has taken a position in the shares and will benefit if the price increases or decreases). To investigate, ASIC has to trace the postings back to the source" [5], [6].

The Committee's subsequent (March 2004) Report did not recommend that ISPs be required to log and maintain records of Internet users' activities [8].

In relation to telecommunications interception powers, we note that ASIC informed the PJCACC on 21 July 2003 that it did not have any need for greater powers to obtain digital evidence by way of warrants:

> "**CHAIR**−Is the question of search warrants a problem in this area? I notice it has been used in terms of the evidence.
> **Mr Inman**−So far ASIC are not aware of any major problems. Search warrant access powers came under examination in recent times in a couple of matters, and we fared well. The recent amendments via the Cybercrime Act addressed many of our concerns about the execution of search warrants and the obtaining of digital evidence. We do not have any additional concerns to report." [6]

It would be interesting to know what, if anything, occurred during the following 11 months such that ASIC now considers it needs access to the content of undelivered communications by way of search warrant.

Also since 2001, ASIC has been seeking to achieve its objectives concerning ISP logging and record retention by way of an ISP Cybercrime Code of Practice developed by the Internet Industry Association ("IIA") and law enforcement agencies. ASIC informed the PJCACC on 21 July 2003 that "We have spent−as I alluded to earlier−two years, and other agencies have spent a lot of time and resources, providing detailed technical advice [to IIA] as to what our needs are" [6].

AUSTRAC

It appears from publicly available information that AUSTRAC did not call for ISP logging and retention of records about Internet users' online activities during the 2001 PJCNCA inquiry. However AUSTRAC has, since 2001, been attempting to achieve the objective of ISP recording and retaining details of Internet users' activities by way of the above mentioned ISP Cybercrime Code of Practice. AUSTRAC informed the PJCACC on 18 July 2003 that it had "been doing quite a lot of work" with IIA on development of the Code and had provided "detailed input" in relation to requiring ISPs to retain records [7].

IIA Draft Cybercrime Code of Practice

IIA's Draft Cybercrime Code of Practice was issued for public comment on 21 July 2003 (the same day that ASIC appeared before the PJCACC) [10].

The Code seeks, among many other things, to require ISPs to routinely retain logs of all Internet users' online activities just in case an LEA might wish to obtain information in the future.

EFA's 2003 submission to IIA stated, in conclusion, that:

> "The Code fails to take into sufficient account the existing provisions of the *Telecommunications Act 1997* and the *Privacy Act 1988*. Compliance with various provisions of the Code is likely to place an ISP in breach of one or both of those Acts.
>
> The data collection and retention provisions of the Code seek to establish a de facto extension of the telecommunications interception regime, enabling access to vastly more communications and personal information than results from telephone call

> intercepts under warrant, without any provisions ensuring accountability, transparency and judicial and Parliamentary oversight.
>
> No information has been provided to the public or the Parliament to even suggest that the problems allegedly being dealt with are sufficiently serious to warrant the massive invasion of Internet users' privacy that would result." [11]

As at 12 July 2004, the draft Code has not been finalised and implemented. We understand that IIA decided to reconsider various aspects following receipt of public submissions.

References

Parliamentary Joint Committee on The National Crime Authority ("PJCNCA"), Inquiry into the Law Enforcement Implications of New Technology, 2000−2001

1. PJCNCA Public Hearing, 2 April 2001 (includes ASIC)
   http://www.aph.gov.au/hansard/joint/commttee/j4734.pdf

2. PJCNCA Public Hearing, 26 March 2001 (includes IIA − references to ASIC submission)
   http://www.aph.gov.au/hansard/joint/commttee/j4733.pdf

3. PJCNCA Report, 27 August 2001
   http://www.aph.gov.au/senate/committee/acc_ctte/itlaw/report/report.pdf

4. EFA Submission, April 2001
   http://www.efa.org.au/Publish/ncasub.html

Parliamentary Joint Committee on the Australian Crime Commission ("PJCACC"), Inquiry into recent trends in practices and methods of cybercrime, 2003−2004

5. ASIC Submission, May 2003
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/submissions/sub5a.pdf

6. PJCACC Public Hearing, 21 July 2003 (includes ASIC and EFA)
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/hearings/210703.pdf

7. PJCACC Public Hearing, 18 July 2003 (includes AUSTRAC)
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/hearings/180703.pdf

8. PJCACC Report, 24 March 2004
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/report/index.htm

9. EFA Submission, 30 April 2003 & Supplementary Submission, 6 August 2003
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/submissions/sub04.pdf
   http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/submissions/sub4a.pdf

IIA Draft Cybercrime Code of Practice

10. Internet Industry Association Submission to PJCACC, 8 September 2003
(contains media release of 21 July 2003 announcing issue of Draft Code of Practice for public consultation and a copy of the Draft Code)
http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/submissions/sub30.pdf

11. EFA submission to IIA re Draft Cybercrime Code of Practice, 19 August 2003
http://www.efa.org.au/Publish/efasubm−iiaccc.html

Attachments

Appendix 1: Extracts from PJ Committee Hansard and Reports

Appendix 1: Extracts from PJ Committee Hansard and Reports

1. **Parliamentary Joint Committee on The National Crime Authority, Inquiry into the Law Enforcement Implications of New Technology**, 2000−2001

1.1 **Public Hearing 26 March 2001 − PJC on the NCA**
http://www.aph.gov.au/hansard/joint/commttee/j4733.pdf

> **Ms Salier** [General Counsel, UUNET and OzEmail Internet; and Representative, Internet Industry Association] −
> ... The submission of the Australian Securities and Investments Commission, ASIC, included extensive references to what they think ISPs should be obligated to do. ASIC called for various areas to be addressed. At page 48 of volume 1 of the submissions, ASIC expressed their concern that there was no present general law to require ISPs to retain records. ASIC suggested that the Proceeds of Crime Act 1987 was a good model for retention to be applied−that is, there were certain specified records that the industry would have to retain for a certain period of time, with penalties applying in the event of failure to comply. At page 49 of volume 1 of the submissions, they suggested that there should be some compulsion for monitoring by ISPs of their subscriber's activities. Again, the Proceeds of Crime Act 1987 was cited as a model in this area. Under division 3 of part 4 of that act, an order may be applied to direct a financial institution to monitor all transactions conducted through a certain account of one of its customers. Again at page 49, there was a suggestion that agencies should be empowered to require the removal of illegal Internet material and serve notices to stop ISPs providing services to customers. The notices to stop providing services in this case were for people that were found to be in contravention of the Corporations Law.
> ...
> Obviously a plethora of issues have been raised for the industry by these submissions including, in relation to privacy, technology capability, costs, enforcement and so on. A common theme through all of the submissions relates to the retention of records. It is interesting to note that at no stage do any of the submissions attempt to define exactly what the records are that they are requiring the ISPs to maintain. If you look at the submissions and transcripts, the term 'records' is referred to in a wide variety of ways. For example, ASIC refers to records as 'the details of communications that have taken place and the parties to the communications'. At the same page, ASIC also refer to log records of proxy servers as being records for the purposes of their discussion. The WA police refer to records as being specific logs and other information relating to the use of ISP systems that may be required to identify those involved in criminal activities.
> ...
> Depending on how that word 'records' is defined results in a dramatic difference in impact on industry, privacy and community. For example, if we take the broad use of the word as given by the ASIC, it is akin to asking a carrier to record every telephone conversation made over its system or asking Australia Post to photocopy every letter that passes through its office. This is not an overdramatic analogy. An ISP does not have an interest in recording or monitoring what its customers do once access is gained to the Internet, except for the purposes of providing its service obviously. ISPs do not track or monitor customer activities or communications. ISPs do not record and maintain such information. There are very good reasons for this.
> ...
> A number of other issues are raised in the submissions. The only one that I will

specifically address is ASIC's suggestion that ISPs should be made to monitor customer activities in certain instances. We would submit that ASIC is de facto suggesting an extension of the interception of communication regime currently governed by the Telecommunications (Interception) Act.This act has also been the subject of discussion within the submissions and the proceedings of this committee. The focus has been on the need for balance and accountability when distributing such powers. Needless to say, the IIA is fully supportive of the concept of the need for balance and accountability for agencies when seeking to use such powers. Interception of communications is a drastic power to bestow, as it necessarily involves a complete invasion of privacy. Powers such as these should only be available on a last resort basis and under stringent guidelines. In fact, the IIA vigorously opposes any extension of such powers beyond the act in which they currently lie.

1.2 **Public Hearing 2 April, 2001 − PJC on the NCA**
http://www.aph.gov.au/hansard/joint/commttee/j4734.pdf

Mr Inman [ASIC]−I think, as a general statement first, by and large the laws that we utilise and the powers that we utilise are sufficient to deal with the new economy as in the old economy. However, there are some aspects where we need to supplement, we believe, the powers that we do have specifically to deal with variations about how online investigations can be conducted, as opposed to how they were conducted in the offline environment.

CHAIR−Do you want to expand on that?

Mr Inman−For instance, a common form of conduct that we come across in our surveillance activities is false and misleading bulletin board postings in relation to securities on the Internet and the use of spam emails to affect market manipulations and pyramid schemes, for instance. ...
...
Mr Inman−... Examples are where people will use the World Wide Web technologies to access a large consumer base cheaply or use false and misleading information to encourage people to purchase investments that do not exist or shares that do not warrant the purchasing of that. The same mediums are being used to promote unlicensed financial advice and to provide hot tips. ...
...
CHAIR−You also would have heard me ask the previous witness about relationships with the Internet industry, particularly relationships and practical cooperation with ISPs, and whether there is a need for legislation there or whether industry self−regulation would be adequate and so on. Could you tell us what your experience has been with ISPs when you have needed help or cooperation. What is your view on the legislation?

Mr Inman−By and large, we have found the industry to be very helpful in relation to our enforcement activities. ... I also understand why Internet service providers harbour concerns about the potential for record keeping. For instance, I have been told that one of the largest Internet service providers in America can store logs in relation to an individual server amounting to several gigabytes of data in one day alone for their customer base. I think you can balance that against a number of factors. ... My final comment on that would be to say that there are precedents which show that often an impost on business is necessary to ensure that the robust rule of

law that we have in our Australian society is maintained. The proceeds of crime legislation provides in a number of places examples where government decided that that was the case.

...

Mr Inman− I am not aware of the last part because ASIC per se does not administer the Proceeds of Crime Act or utilise it too often. I do not have any information on that. My comments about the logs was specifically aimed at communication logs.

...

CHAIR−I alluded earlier to the evidence we got last week from the Internet Industry Association witness. The secretary will make sure you get a copy of that because I would be interested in your reaction to what that witness said. Similarly, there was interest, as you heard earlier, in what the AFP's reaction was, but in different areas. I am interested to know your reaction to what they had to say in that privacy area, because part of their argument was that there were major privacy concerns if legislation was passed giving access to bodies like the NCA or others to their systems. They also went into great detail−certainly superficially, very convincing detail−about the quantum required for storage of information. ....I would be interested to have your views on those calculations that they gave us about the cost of them having to keep the sort of records that might be appropriate.

Mr Inman−... Firstly, I realise that it would be a very large impost on certain Internet service providers if it were a requirement that they keep all records forever. Having said that, I am also aware of at least one who does that. I think that if there is to be some form of obligation on Internet service providers, in determining what that length of time is, it should be determined after consultation.

...

CHAIR−Thank you very much for attending this morning. We will make sure we send you what we talked about. The lady who appeared on behalf of that association will probably be surprised that we are asking witnesses to specifically respond. She made some very categorical statements and I think it is important that we hear the contrary view−or possibly contrary view.

1.3 **Report of the Parliamentary Joint Committee on The National Crime Authority, *Inquiry into the Law Enforcement Implications of New Technology***, 27 August 2001
http://www.aph.gov.au/senate/committee/acc_ctte/itlaw/report/report.pdf

"1.57 The Action Group into Electronic Commerce (AGEC), which was formed in 1997 by the Heads of Commonwealth Operational Law Enforcement Agencies to research the impact of electronic commerce on law enforcement, identified that one of the key issues in improving law enforcement's response to changing information technology as being 'facilitating appropriate record keeping standards for Internet Service Providers'.

1.58 Several members of AGEC addressed this issue in their individual submissions to this inquiry ...

...

1.62 The Australian Securities and Investments Commission (ASIC) also submitted its concerns about the need for better regulation of ISPs. Its submission foreshadowed that the Financial Services Reform Bill − to modernise the regulation of the Australian financial services industry − would also give ASIC some additional enforcement powers to combat computer crime. At the time of preparation of the ASIC submission, it was thought that the Bill would contain provisions to permit ASIC to serve a written notice requiring a person providing services as an ISP to

maintain log records created during a specified period of time. It also drew attention to several other proposals expected to be in the Bill, such as a provision to enable it to make mirror images of hard drives of computers during the execution of search warrants and a provision enabling it to serve on an ISP a written notice requiring it to immediately cease providing services where information is placed on the Internet in contravention of the Corporations Law. [48]

> [Footnote 48: The *Financial Services Reform Bill 2001* was introduced into the House of Representatives on 5 April 2001. The issues foreshadowed in ASIC's submission were not included in the Bill.]

1.63 ASIC also ... suggested that, following the precedent of the *Proceeds of Crime Act 1987*, provision be made for law enforcement to be able to seek a Supreme Court order to require ISPs to monitor transactions through a customer's account.
...
1.67 AGEC subsequently submitted a clear statement of the position taken by law enforcement... In summary, AGEC stressed that there was no question of seeking records regarding the content of communications, since this was already covered by the provisions of the TI Act."

2. **Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into recent trends in practices and methods of cybercrime*,** 2003 − 2004

2.1 **Public Hearing, 21 July 2003 − PJC on ACC**
http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/hearings/210703.pdf

Mr Inman [ASIC]−...When we take a proactive stance−that is, we try to identify an offence while it is still being perpetrated; a classic example is when a web site suddenly appears offering someone an investment, the content of which contravenes our legislation−we need to find out who is behind that. The types of material that we are dealing with when we do that are not paper based; they are very much logs−computer logs, network logs−and those types of things. Our submission highlights the fact that, as a regulator undertaking an enforcement investigation, we rely very much on the logs and the computer records of non−government entities. That is where most of the information infrastructure is; it is in private hands. As we start to trace our way through that technology to the source of the offending material, we are dependent on companies, telecommunications carriers and Internet service providers to have logs operating.
...
Mr Inman−It is very cooperative. We have spent−as I alluded to earlier−two years, and other agencies have spent a lot of time and resources, providing detailed technical advice as to what our needs are. The Internet Industry Association has welcomed that. It might not meet all of our needs but, as I said earlier, there has been good faith shown by the Internet Industry Association, and there will be cost implications for the industry participants on this−there is no doubt about it. So they are taking their share of the load.
...
CHAIR−Is the question of search warrants a problem in this area? I notice it has been used in terms of the evidence.
Mr Inman−So far ASIC are not aware of any major problems. Search warrant access powers came under examination in recent times in a couple of matters, and we

fared well. The recent amendments via the Cybercrime Act addressed many of our concerns about the execution of search warrants and the obtaining of digital evidence. We do not have any additional concerns to report.

2.2 **Public Hearing 18 July 2003 − PJC on ACC**
http://www.aph.gov.au/senate/committee/acc_ctte/cybercrime/hearings/180703.pdf

> **Ms Atkins** [AUSTRAC]− ... Also in terms of the sorts of things you are talking about−monitoring and keeping records−one of the big problems for law enforcement, if somebody is, say, using the Internet to conduct transactions, is: how long are the records kept and how can they get at them? We have been doing quite a lot of work with people like the Internet Industry Association, who have developed a code into which, through AGEC, we have given detailed input about how long they are prepared voluntarily to keep information. ...