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

30 May 2005

Committee Secretary
Senate Legal and Constitutional References Committee
Department of the Senate
Parliament House
Canberra ACT 2600

Via Email: legcon.sen@aph.gov.au

Dear Sir

Inquiry into the *Privacy Act 1988*

We enclose herewith supplementary submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Supplementary Submission

To: Senate Legal and Constitutional References Committee
Re: Inquiry into the *Privacy Act 1988*

30 May 2005

Contents:

---

1. Preamble

1. EFA appreciates the opportunity provided by the Committee to submit information in relation to commentary in Hitwise's submission of 21 April 2005 referring to EFA's submission of 24 February 2005.

2. We advise that we do not have any further comments in relation to the Hitwise software that operates within some ISPs' networks. Obviously organisations such as EFA and other members of the public are not able to know details of the operation of proprietary software and patent pending commercially and competitively sensitive technology that is not available for public use and/or analysis. Comments in our previous submission in that regard were based on publicly available information from the Hitwise website and newspaper reports, as we believe we made clear in that submission.

3. In this document, we address comments made by Hitwise concerning EFA's submissions in relation to IP addresses and the definition of personal information.

4. We also take this opportunity to re−iterate our advice during the hearing on 22 April 2005 that we have not published our submission to the Committee dated 24 February 2005. In that regard the Hitwise submission states that there is a "version" of that submission on EFA's web site. That is not a fact. It is probable that Hitwise may have viewed EFA's submission dated 22 December 2004 to the Federal Privacy Commissioner's review of the *Privacy Act 1988*, a copy of which is on EFA's web site. Following our completion of that submission, there was then a two month period in which to prepare and lodge a submission to the Committee's inquiry. As we therefore had time to consider and research a number of additional matters, and the terms of reference of the Committee's inquiry are different and broader, our submission to the Committee's inquiry is quite different. It contains additional information on some matters and also information on numerous other matters that were not mentioned in our submission to the Federal Privacy Commissioner's review.

▲ Go to Contents List

2. IP Addresses and Personal Information

5. We note the following remarks in Hitwise's submission:

> "*IP addresses are not considered to be 'personal information' as they do not identify a person. However, EFA appears to be claiming that an IP address can be said to identify 'some individuals' and that it should be regarded as 'personal information'. It is not clear why EFA has formed this view.*" (Page 2)

6. We take this opportunity to advise the Committee that EFA has formed the view that IP addresses should be legislatively regarded as "personal information" because it is a fact that IP addresses can be, and are being, used to identify individuals.

7. As OzEmail's General Counsel, Ms Mary−Jane Salier, informed the Joint Committee on the National Crime Authority[1] in March 2001:

> "*[O]ften police investigations start with an IP address as opposed to a user ID. Therefore, you have to work backwards to find out who you allocated the IP address to and at what time in relation to user records.*"

8. Other regulatory and enforcement agencies, such as the Australian Securities & Investments Commission ("ASIC"), also start with an IP address. Details of how ASIC uses an IP address to identify an individual who has posted illegal investment advice to a web site bulletin board is available in Case Study A of *Investigating Internet Fraud*[2], an ASIC presentation to the 4th National Investigations Symposium in November 2002, by Keith Inman−Director and David Perry−Legal Counsel, Electronic Enforcement, ASIC.

9. Details of how ISPs "work backwards" from an IP address to identify an Internet user, as referred to above, is available in the section titled "How an ISP can identify and monitor/track customer activities" of EFA's supplementary submission to the Joint Committee on the Australian Crime Commission's *Inquiry into recent trends in practices and methods of cybercrime*[3] dated 6 August 2003. Also, the third section of that submission provides information about identification of individuals from IP addresses contained in the header fields of email messages they have sent (whether from a free email account or not).

10. We wish to make clear that we are **not** suggesting that enforcement agencies should be prohibited from obtaining and using IP addresses to identify individuals. Our point is that enforcement agencies would not be using IP addresses in the course of their investigations if IP addresses could not be used to identify individuals.

11. Since plainly IP addresses can be, and are being, used to identify individuals, but some businesses contend that they are not "personal information", we consider that the definition of "personal information" in the Privacy Act needs to be amended to unambiguously cover IP addresses.

12. EFA acknowledges that Hitwise has advised the Committee that:

> "*To elaborate, partners ISPs use proprietary software provided to them by Hitwise to extract aggregate data from their proxy caches. This may involve the software 'analysing' the IP addresses that are included within proxy caches. As noted above,*

IP addresses are not considered by Hitwise to be 'personal information'. Nevertheless, Hitwise wishes to emphasise that this process is conducted within the ISP's network (using the proprietary software), not at Hitwise, and no IP address information or personal information is disclosed to Hitwise." (Page 3)

13. However, as Hitwise does not consider IP addresses to be personal information, it would appear to follow that, if ISPs did disclose IP addresses and details of web pages visited to Hitwise, Hitwise would not consider that disclosure by ISPs nor collection by Hitwise to be in breach of the Privacy Act.

14. It is precisely because some organisations do not consider IP addresses to be personal information that EFA is of the view the IP addresses should be clearly covered by the definition of personal information. While it remains unclear whether they do constitute personal information as defined in the Act, it also remains unclear whether or not the Privacy Act prohibits ISPs, and businesses that host web sites, from disclosing information about individuals' online activities (e.g. web browsing) to another business, and if it does not, then it also does not prohibit that other business from disclosing the information to yet another business.

15. In terms of protection of privacy, it is irrelevant whether the business to whom the information is disclosed can ascertain the identity of individuals from that information alone. On the Internet, it is not necessary for businesses to be able to reasonably ascertain the actual identity of an individual, in order to build a profile about them. All that is necessary is a sufficiently unique identifier. Such identifiers (and profiles) may then be disclosed to other businesses/entities who *are* able to connect a 'cyberspace' identifier with a name or other 'real−world' identifier such as an individual's name.

16. In our view, information involving IP addresses from proxy server and web server logs, etc, should not be permitted to be disclosed except as required by a warrant issued to law enforcement agencies or as required by a court order.

▲ Go to Contents List

3. ISP use of IP addresses

17. It should be noted that many, arguably all, IP addresses recorded in an ISP's proxy cache/log are unquestionably personal information when in the possession of the ISP. It is the ISP who allocates an IP address to a customer when the customer logs in. Therefore, ISPs can easily ascertain which customer account was connected to the Internet via a particular IP address at any point in time by checking their log in records. In cases where only one individual uses the particular account, the IP address enables identification of that particular individual. In cases where, for example, a family uses the same account, the IP address enables the identification of the member of the family who opened the account.

18. In cases of only one individual using an account, an ISP's **use** of IP addresses (which identify the individuals who visited particular web pages etc) in the course of analysing and extracting information from their proxy caches for the secondary purpose of providing information to an unrelated organisation for that other organisation's own business needs appears likely to be in breach of NPP 2.1. NPP 2.1 prohibits **use** or disclosure of personal information unless both "the secondary purpose is related to the primary purpose of collection" (and directly related if sensitive information) and "the individual would reasonably expect the organisation to **use** or disclose the information for the secondary purpose". The secondary purpose is not related to the primary

purpose of providing Internet access, and EFA considers it highly likely that many Internet users would not expect their ISP to be using their IP address/personal information and details of web browsing activities for such a secondary purpose.

▲ Go to Contents List

4. Consistency with OECD countries

19. In relation to privacy laws that are in place overseas, Hitwise states that:

> "*'Personal information' is consistently described as information or data that can be used to identify an individual. EFA have not presented any sound policy reasons why Australia should adopt laws that are inconsistent with other OECD countries that have enacted privacy legislation.*" (Page 4)

20. We wish to draw to the Committee's attention that the change advocated by EFA concerning IP addresses being covered by the definition of "personal information" would not be inconsistent with various other OECD countries, according to a 2004 research report, commissioned by the U.K. Information Commissioner, titled *What are 'Personal Data'?*[4].

21. The U.K. researchers conducted surveys asking data protection authorities in various countries, among other things, what types of information/data were considered to be "personal information" or "personal data" (as applicable) under the law of their country and whether the data types were always, sometimes, or never considered to be personal data. One type of data asked about was 'Computer IP Address'. The research found that computer IP addresses were always considered to be personal data by 40% of the countries surveyed (Graph 1, page 62). In the case of the subset consisting of EC member countries, 60% said computer IP addresses were always considered to be personal data (Graph 3, page 69).

22. We also note that Australia's definition of "personal information" is currently inconsistent with all other countries surveyed. It is the only one that refers to information about an individual "whose identity is apparent, or can reasonably be ascertained" from the information. EFA considers the "can reasonably be ascertained" aspect of the Australian definition to be problematic because the definition begs the questions: reasonably ascertainable by whom? and does whether it "can reasonably be ascertained" depend on how much time or effort needs to be devoted to ascertaining the individual's identity? In contrast, half of the 18 countries surveyed have definitions that refer to information "relating to" or "concerning" "an identified or identifiable" individual, or "an identifiable" individual. This may be why, in 60% of the EC member countries surveyed, IP addresses are always considered to be personal data.

23. Furthermore EFA sees no reason why Australia should not take a lead in endeavours to adequately protect the privacy of Internet users, as it did for example in enacting the *Spam Act 2003*.

24. Also, consideration of the need to change definitions of personal information to adequately protect privacy is not only occurring in Australia. For example, the Federal Privacy Commissioner's Report *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*[5] quotes a December 2004 research paper prepared for the Council of Europe[6], on the application of data protection principles to the world wide telecommunications networks, which states:

"*The advent of the Internet has created a need for a third generation of data protection regulations*"

25. The Federal Privacy Commissioner's Report states:

"*As the Council of Europe research suggests:*

'*New technology makes it increasingly possible to process data relating to individuals not, as was traditionally the case, through data relating to their legal identity, such as name and address, but via an anchor point or even an object (so−called ambient intelligence) associated with it. This means that the danger often no longer resides in the collection of personal data as such but in the subsequent application of abstract profiles to individuals.*'

The European research report says that it is clear that the Consultative Committee will have to work with the concept of personal data. It concludes:

'*A definition of personal data based on undefined and indefinable notion of identity and the pendant concept of anonymity is ambiguous and not directly workable. From the practical point of view, it would be better to refer to biographical data, identifiers linked to individuals or to terminal (indeed objects), and points of contact.*'"

26. If Australia was to take a lead in the next generation of data protection regulations, it may need to act soon given other countries are also considering the matter and some already regard computer IP addresses as always being personal information.

▲ Go to Contents List

5. Anonymisation/de−identification of information in the Internet age

27. The U.K. report referred to above, *What are 'Personal Data'?*, is of itself an example of the dangers inherent in attempting to anonymise/de−identify information before making it available to other people and/or businesses in the Internet age.

28. Questionnaire 2 sent to data protection authorities stated that *"We will ensure that in the final report and any subsequent publications resulting from this work, the data is anonymised by not referring to any country or individual by name".*

29. In the final report the countries are referred to by numbers, e.g. "Country 36" and divided into three groups (Group 1, the eight participants in the EU; Group 2, seven jurisdictions outside the EU, but wishing to comply with the Directive for trade purposes or requiring compliance for accession; Group 3, three countries outside the EU with no requirement of compatibility). Appendix 1 of the report contains a list of the countries by number together with the definition of personal data in each of the numbered countries.

30. However, merely entering a definition into a search engine such as Google provides a high probability of correct identification of some countries, particularly when combined with the information about which of the three groups that country is in. For example it is highly likely that

the countries in Group 3 are Australia (36), Canada (37) and New Zealand (40). Canada is also more than likely to be Country 37 given the reference to Country 37 and the "Canadian position" on page 103.

31. Given Australia's highly unusual definition of "personal information", and footnote 120 which refers to Country 36 and an Australian court decision, it appears beyond doubt that Country 36 is Australia. According to the information on pages 143 and 146 of the report, the data protection authority in Country 36 said that IP addresses were "sometimes" considered to be personal information, as were all other types of data except a 'National registration number'. The report also states that "Country 37 [probably Canada] and Country 36 placed more than 90% of data types in opposing categories (always and sometimes respectively)" (page 67).

32. In summary, the report shows that it is much more difficult to reliably anonymise/de−identify information in the Internet age than it was in the past, and, Australia's position on what is, or is not, always "personal information" is not consistent with that of other countries.

33. While there are also considerable differences among other countries, Country 36 (Australia) and Country 12 were found to be the "most extreme examples" of where all (or most of) the data types are only 'sometimes' capable of being personal data, in contrast to other countries where more types are 'always' personal data.

34. In EFA's view, Australia's definition needs to be changed so that the Australian position ceases to be the most extreme in the above regard, in order to provide improved protection for individuals' privacy.

▲ Go to Contents List

6. Impact of definition on ISPs and other businesses

35. We note that Hitwise contends that:

> "*a change of kind advocated by EFA would be likely to have very significant implications for the Internet industry and e−commerce...it could impact upon the operation of proxy caches...and upon the type of network monitoring that every ISP conducts... Furthermore, inclusion of an IP number in the definition of personal information would negatively impact on the business processes of every company with an Australia website*"

36. The change advocated by EFA would not have such an impact. The Privacy Act does not prevent ISPs and other businesses from collecting personal information that is necessary for their own business needs, nor using it for their own business needs. Such a change would only prevent them from disclosing the information to other businesses for secondary purposes that are not related to the primary purpose for which they collected the information, and they would be permitted to do even that with the consent of the relevant individuals.

37. EFA considers individuals should have a choice about how information about them is used and disclosed. Prohibition on disclosure without consent is especially important in circumstances where individuals have no choice about whether information about them is collected in the first place. The slogan adopted by the Federal Privacy Commissioner in relation to the private sector provisions is "My Privacy, My Choice". However, individuals have no choice about whether they leave personal

information and related data trails in proxy caches and/or web server logs, etc, other than not to use the Internet. Therefore EFA is of the view that use and disclosure of such information should be strictly regulated to prevent disclosure without consent, except for legislatively specified permitted purposes such as as when required by a warrant or a court order.

▲ Go to Contents List

References

1. Joint Committee On The National Crime Authority, Inquiry into the Law enforcement implications of new technology, Committee Hansard, 26 March 2001.
<http://www.aph.gov.au/hansard/joint/commttee/j4733.pdf>

2. *Investigating Internet Fraud*, Keith Inman−Director and David Perry−Legal Counsel, Electronic Enforcement, Australian Securities & Investments Commission, Presentation to the 4th National Investigations Symposium, 7 & 8 November 2002.
<http://www.security.iia.net.au/downloads/investigating_internet_fraud.pdf>

3. EFA's Supplementary Submission to the Joint Committee on the Australian Crime Commission's *Inquiry into recent trends in practices and methods of cybercrime*, 6 August 2003.
<http://www.aph.gov.au/Senate/committee/acc_ctte/completed_inquiries/2002−04/cybercrime/submissions/sub4a.pdf>

4. *What are Personal Data: A study conducted for the UK information Commissioner*, by Sharon Booth, Richard Jenkins, David Moxon, Natasha Semmens, Christopher Spencer, Mark Taylor, The University of Sheffield, 2004.
<http://www.informationcommissioner.gov.uk/cms/DocumentUploads/What%20are%20personal%20data%20re

5. *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, Office of the Privacy Commissioner, March 2005.
<http://www.privacy.gov.au/act/review/index.html>

6. *Report on the Application of Data Protection Principles to the worldwide telecommunication networks: Information self−determination in the internet era; thoughts on Convention No. 108 for the purposes of the future work of the Consultative Committee (TPD)*, Council of Europe Strasburg, 13 December 2004.

▲ Go to Contents List