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

24 February 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/Madam

Inquiry into the *Privacy Act 1988*

Please find attached submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

EFA appreciates the opportunity to make a submission and would be pleased to provide further information, including by way of oral testimony, in response to any questions Committee members may have.

EFA's Executive Director is based in Brisbane and can be contacted directly at the telephone and fax numbers shown above and by email to ed@efa.org.au. In the event that the Committee may wish to ask EFA to attend a hearing, with a view to assisting the Committee Secretariat in scheduling hearings, we advise that the most convenient venues for EFA are, in order of preference, Brisbane, Canberra, Sydney and Melbourne. We generally prefer, if convenient to the Committee, an early afternoon session so that if an EFA representative needs to travel from interstate, this can be done on the day of the hearing, in order to minimise travel costs, rather than requiring an overnight stay due to airline flight schedules (particularly during daylight saving months).

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA) Submission

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

24 February 2005

Contents:

---

1. Executive Summary

a. The *Privacy Act 1988* as amended fails to adequately protect and enforce individual privacy, creates a confusing regulatory environment and needs to be replaced.

b. The current legislative regime does not adequately protect the privacy of Australians in relation to technologies that have been in use for a decade. It certainly does not have the capacity to respond adequately to new and emerging technologies that have implications for, and/or facilitate invasion of, privacy.

c. A broader definition of "personal information" must be embraced in order to more adequately protect individuals' privacy in the electronic information age. Identifiers such as an Internet user's machine ID, IP address, user ID, email address, passwords, etc. must be clearly incorporated within "personal information".

d. Information about Internet users' activities and behaviours is currently being collected, used and disclosed in ways that consumers are unlikely to have consented to or even be aware of.

e. The commencement of the *Privacy Amendment (Private Sector) Act 2000* resulted in a reduction in regulatory privacy protection in respect of telecommunications businesses.

f. Inconsistencies between the privacy protection provisions of the *Telecommunications Act 1997* and the *Privacy Act 1988* need to be removed so that, among other things, neither Act unnecessarily authorises breach of the privacy protection afforded by the other Act.

g. Lack of enforcement and questionable interpretation of some provisions of the *Telecommunications Act 1997* are enabling ongoing breaches of the privacy protection provisions of that Act (and these breaches are also contrary to the NPPs). For example, in relation to disclosure and use of silent and other blocked calling number information and personal information recorded in the Integrated Public Number Database.

h. Relatively new technologies have given rise to a "vacuum cleaner" approach to computer searches. Discovery processes in civil litigation, in particular Anton Piller orders, are being used in ways that breach the privacy of uninvolved third parties. Changes to court rules or practices are required to ensure appropriate protection of the privacy of third parties, especially when information is indiscriminately seized via a "vacuum cleaner" approach.

i. The roll out of smart cards by government has an extremely high potential to result in a de facto Australia Card, whether or not that is the government's intention at the outset. This risk arises from a combination of factors including the ease with which smart cards can be used for two−way communication with a centralised database and that smart card technology is designed to facilitate function creep. Both the insecure Medicare smart card and the proposed multi−purpose Queensland Driver Licence smart card are of major concern.

j. There are security and privacy risks inherent in use of smart card technology. While smart cards may be tamper−resistant, they are not tamper−proof.

k. The lack of legislative controls on use of radio frequency identification chips (RFID, Contactless Integrated Circuits, etc), is of serious concern in relation to implantation in

human beings, in documents that individuals are required to carry and in clothing and other consumer goods. Laws such as the *Australian Passports Act 2005* which require individuals to carry devices that "broadcast" their identity information are inherently dangerous.

l. A recent court decision shows the need for amendment to IPP 12 "Storage and security of personal information", which applies to the government sector, to require technological access controls on government databases to prevent unnecessary access to (and subsequent disclosure of) personal information by public servants.

m. The exemptions for small businesses, related bodies corporate, political parties and direct marketing without consent should be deleted.

n. NPP 2 should be amended to regulate use and disclosure of information collected for the primary purpose of collection as there is no legitimate reason for NPP 2 to apply only to use and disclosure for secondary purposes. NPP 2 should also be amended to explicitly place restrictions on use and disclosure by secondary collectors, that is, organisations that have collected personal information from another organisation.

o. The common business practice of requiring bundled "consent" and providing NPP 1.3 information in privacy policies that are changeable without notice are undermining the objectives of the *Privacy Act 1988*. Amendments should be made to these principles and also to NPP 3 (data quality) so that it cannot be used as an excuse for using bundled consents.

p. The NPPs should be amended to clearly prohibit knowingly collecting unlawfully disclosed information and close related loopholes concerning unlawfully disclosed information, and also to require that collection be for a lawful purpose.

q. NPP 8 needs to be amended to clarify that the anonymity obligation is to wherever possible (lawful and practicable) facilitate anonymous transactions, including with other businesses.

r. NPP 9 should be amended to ensure that individuals' privacy is adequately protected where information is to be sent to a foreign country and/or customer enquiry/support centres are located overseas.

s. A number of other NPPs need to be amended to close presumably unintended loopholes and/or remove ambiguity.

t. Additional enforcement mechanisms are required. The Commissioner should be given additional powers, particularly in respect of obtaining enforceable undertakings, issuing binding codes, enforcing compliance where a breach has been found as a result of his or her 'own motion' investigation and proactively auditing private sector compliance.

u. Complainants and organisations should have the right to appeal against the Commissioner's determination to the Administrative Appeals Tribunal to have the matter heard afresh.

v. Additional funding should be provided to the OFPC to enable dealing with complaints promptly, and without needing to remove staff from other important areas such as policy and auditing of government agencies as has reportedly occurred.

Go to Contents List

2. About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non−profit national organisation representing Internet users concerned with on−line rights and freedoms. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act* (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities. The role of Executive Director was established in 1999 and reports to the Board.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. EFA's Executive Director was an invited member of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and the Research Reference Committee (2001) and the Privacy Consultative Group (2004−2005). EFA participated in NOIE's Privacy Impact Assessment Consultative Group relating to the development of a Commonwealth Government Authentication Framework (2003), in Centrelink's Voice Authentication Initiative Privacy Impact Assessment Consultative Group (2004) and the ENUM Privacy and Security Working Group convened by the Australian Communications Authority (2003−2005). EFA has presented written and oral testimony to Federal Parliamentary Committee and government agency inquiries into privacy related matters, including amendments to the *Privacy Act 1988* to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.

▲ Go to Contents List

3. Introduction

Overall Effectiveness and Appropriateness of the Privacy Act 1988

1. In 2000 EFA informed two Parliamentary inquiries that EFA did not support the *Privacy Amendment (Private Sector) Bill 2000*, in the form proposed, because the Bill contained too many exemptions and exceptions and failed to come to grips with consumer privacy needs in the 21st century. The Bill was at best a token attempt to introduce privacy legislation.

2. Among many other things, we remarked that the definition of "personal information" is inadequate in context of the electronic environment; that the exemption for small business would introduce a confusing and complex regulatory environment that fails to protect consumers from privacy invasive practices; and that enforcement provisions are inadequate.

3. Our experience since the private sector provisions commenced has shown that our concerns were well founded.

4. Instead of empowering individuals to exercise their right to privacy of personal data, the private sector provisions have conferred on business interests the right to invade individual privacy.

5. We had hoped that NPP Guidelines to be issued by the Privacy Commissioner would assist towards clarifying the complex, unwieldy and ambiguous nature of the NPPs and we were generally supportive of the draft guidelines issued for public consultation in 2001. However, subsequently the draft guidelines were gutted after heavy lobbying by big business.

6. In the absence of comprehensive guidelines, there is no impediment whatsoever to some businesses and regulators interpreting the NPPs in the least privacy protective way possible. In our view some interpretations being used are contrary to the intent and objectives of the legislation and contrary to what many individuals would expect from reading the NPPs.

7. In 2000 we considered the private sector provisions needed to be re−drafted, preferably as a replacement for, rather than an amendment to, the *Privacy Act 1988*[1].

8. We remain of the view that the *Privacy Act 1988* as amended needs to be replaced with a new Act that makes a genuine attempt to protect individuals' privacy.

9. In the remainder of this submission, we comment on a number of aspects of particular concern. However, we stress that we do not believe that patching the existing legislation will result in adequate privacy protection.

10. Furthermore, a lack of comment on any particular issue in this submission should not necessarily be taken to mean that EFA has no concerns in that regard. There are too many problems with the provisions of the legislation to document them all herein. We would be happy to advise our view concerning any particular issue not mentioned herein on request from a Committee member or Secretariat staff.

▲ Go to Contents List

4. Capacity of the Current Legislative Regime to Respond to New and Emerging Technologies

11. The current legislative regime does not adequately protect the privacy of Australians in relation to technologies that have been in use for a decade. It certainly does not have the capacity to respond adequately to new and emerging technologies that have implications for, and/or facilitate invasion of, privacy.

4.1 Telecommunications including the Internet

4.1.1 Reduction in Privacy Protection since 2001

12. Telecommunications carriage service providers were one of the first groups of private sector businesses required to comply with privacy protection legislation, as the government and Parliament recognised the need for telecommunications privacy over a decade ago. The current privacy

protection provisions in Part 13 of the *Telecommunications Act 1997*[2] ("TA") are substantially the same as those previously contained in the *Telecommunications Act 1991*.

13. However, new telecommunications−based services and technologies together with much larger numbers and types of telecommunications service providers have undermined the privacy protections of the TA. In addition, some exceptions to the privacy provisions of the TA are now being used in ways that are most unlikely to have been envisaged or intended by the government and Parliament when enacting them in 1991/92 to facilitate the introduction of competition in the telephone call services market.

14. Although it may generally be assumed that the *Privacy Amendment (Private Sector) Act 2000* would have increased privacy protection, this is not the case in relation to some sections of the telecommunications industry. In fact, several events associated with the commencement of the private sector provisions of the PA have resulted in circumstances where individuals have less privacy rights than previously in relation to businesses in the telecommunications sector, and also less than in relation to non−telecommunications businesses that are required to comply with the PA. Those events include:

- insertion of then new Section 303B into the TA which states that exceptions to the Part 13 privacy protections of the TA are taken to be "authorised by law" for the purposes of the PA;

- de−registration by the Australian Communications Authority ("ACA") on 21 December 2001 of the previously enforceable[3] ACIF *Industry Code−Protection of Personal Information of Customers of Telecommunications Providers*[4]. The Code expanded on the privacy protections of Part 13 of the TA and had been enforceable since 1 May 2000. As stated in the Code:

  > "Part 6 of the [Telecommunications] Act sets out the intention of the Commonwealth Parliament that bodies and associations that represent sections of the telecommunications industry should develop codes of practice relating to the telecommunications activities of those bodies and lists key privacy issues as examples of areas where codes may be developed. One area expressly mentioned is the protection of personal information. [113(3)(f) "privacy and, in particular: (i) the protection of personal information;"] ... This Code complements the privacy protection in the Act, and also addresses matters which are not dealt with in Part 13, such as how information should be collected, stored and handled, and how consent and reasonable awareness are to be determined."

- apparent failure to pay due regard, prior to de−registering that Code, to the fact that many small businesses, including in the telecommunications industry, are not required to comply with the PA.

15. Hence there is no longer an industry privacy code as intended by the Parliament when enacting Part 6 of the TA, nor has an industry privacy code been developed as envisaged by the 2001 amendments to the PA.

16. It should also be remembered that the *exceptions* to the privacy protections of the TA apply not only to large telecommunications service providers such as telephone call companies, but also to

small businesses including Internet Service Providers; resellers of carrier and/or ISP services; carriage service "intermediaries"; and telecommunications contractors (s271).

17. In summary, prior to the 2001 Privacy Act amendments an enforceable industry code substantially the same as the National Privacy Principles ("NPPs") applied to all telecommunications service providers including small businesses. The code also limited the breadth of the exceptions to the privacy protection provisions in the TA. However, since 2001, exceptions in the TA have in effect authorised breach of the NPPs (and there is no longer an enforceable code limiting the breadth of those exceptions) and small businesses have not been required to comply with the NPPs nor a substantially similar industry code. Furthermore, some exceptions to the Part 13 privacy protections in the TA are inconsistent with the PA without justifiable reason as discussed in detail in Appendix 1.

▲ Go to Contents List

4.1.2 Current and Emerging Telecommunications Privacy Issues

18. We provide below information about recently emerged privacy issues involving the telecommunications industry and examples demonstrating that existing privacy protection legislation is failing to adequately protect individuals' privacy.

19. Firstly we note the findings of the OFPC's 2004 research showing that:

> *"Individuals' trust is lowest of all in internet [sales] companies (9%). These were intended to particularly benefit from the introduction of the private sector provisions. Trust in internet companies appears to remain unchanged since 2001. Six in ten respondents to the Office's 2004 survey have more concerns about the security of their personal details than usual when using the internet and this level of concern has risen since the 2001 study."* (OFPC Issues Paper, p26[5])

20. We find the results of the OFPC research concerning lack of trust in the online environment, not only completely unsurprising, but also justified.

21. The OFPC Issues Paper (p27) goes on to suggest that the lack of confidence may be due to "a lack of awareness about privacy rights [that] has prevented people from developing a clear and concrete sense of confidence that their privacy rights are protected" and seeks suggestions concerning ways that the OFPC, or others, can encourage community confidence that privacy rights are protected online.

22. EFA considers that any attempt by the OFPC or others to encourage the community to believe that their privacy "rights" are protected online would be highly misleading at best. The fact is that, under existing Australian law, individuals have almost no privacy "rights" in the online environment and even the few privacy rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced.

23. The lack of rights and/or adequate protection of rights arises from a combination of factors, including but not limited to, uncertainty regarding the definition of "personal information"; no requirement to obtain consent before collecting personal information; use of bundled "consents" including to disclose information to unspecified "partners"; the small business exemption; and/or technological developments.

24. Before the private sector provisions commenced, it was no secret that, for example, Internet service providers have access to huge amounts of personal information. As pointed out in May 2000 by the then General Manager of OzEmail ISP in a paper presented to an IIR Privacy Law Conference[6]:

> *"...And here's the somewhat scary bit. We [OzEmail] have the username and password for every one of our users; we have their credit card details, we have a lot of information about their liquidity, we can know about every purchase they make online, with whom, when and for how much. We can know every site they visit on the web − every page, every newsgroup, every picture they look at. We could read all of their mail and know all about their romances and the jobs they're applying for.*
>
> *The commercial opportunities arising from this are endless, of course. We could watch what each of our customers does, and then just pop them a quick email that says, 'Oh − we see that you just bought a nice new pair of brown boots. One of our other merchants just happens to have a special on black socks − just follow this link.' Or 'We see that you've been looking at dirty pictures tonight − in fact the sixth and 10th pictures you looked at were over the top and you're busted.' In short there's not much we couldn't find out about the online life of our customers − and remember, in a few years our customer base will represent a sizeable chunk of the Australian population. A chunk about the size of NSW for example. This is becoming irresistible to both marketers and governments, who often share the view that they have a God given right to access private information about the general public.*
>
> *Then, of course, we could go in for a bit of datamatching, where we instruct our databases to match names, products and addresses with other databases. String three or four conditions together in a query which trawls two or three databases and you get amazing pinpoint clarity. The accuracy of this kind of targeting truly provides the so called 'market of one'. And the nature of the net means that the marginal cost of marketing to the next market of one is effectively zero.*
>
> *And right now in Australia there is almost nothing to stop us from doing this."*

25. At that time ISPs were subject to the limited privacy protection obligations set out in Part 13 of the *Telecommunications Act 1997*. Later, in December 2001, the private sector amendments to the *Privacy Act 1988* commenced.

26. Nevertheless, it has since become apparent that some ISPs are covertly disclosing information about Internet users and their online activities without the consent, or even knowledge, of the subject individuals. Examples are provided below.

▲ Go to Contents List

4.1.3 Examples of Inadequacy of Existing Privacy Legislation

(a) Businesses covertly surveilling Internet users

27. Media reports about the activities of market analysts/researchers give rise to serious questions concerning how, and the extent to which, online users' activities are being monitored, tracked and recorded as a result of disclosure of information about Internet users by ISPs to third party

businesses. For example:

- *Online research a wise hit*, by Louise Hattam, Herald Sun Melbourne (Business, p25), 19 Jul 2004[7]:
  "Each day, Hitwise monitors more than 25 million home, work and educational internet users worldwide. ...
  The company was the first in Australia to obtain its information from internet service providers, rather than the conventional survey methods of market research companies. ...
  'Hitwise gathers information from partner ISP networks and other data sources,' Mr Walsh [Hitwise CEO] said. ...
  The reports [also] show where users have been immediately before and after visiting a site. ..."

- *Bright future for online banking*[8], by Adrian Giles [founder and director of Hitwise], WebHead Magazine, ZDNet Australia, 26 Sep 2001:
  "...Who visits Internet banking sites?
  According to Hitwise demographic data, 57 percent of visitors are men, slightly up on the overall average of 55 percent for all sites. While 18−24 year−olds account for 23 percent of all Internet traffic measured by Hitwise, they supply just 13 percent of traffic to Internet banking sites, showing that younger Australians use the Internet more for education and entertainment purposes than they do for paying bills and accessing their banking details. Online banking is particularly popular with the 25−34 age group, who supply 33 percent of visits to Internet banking sites. ...
  Adrian Giles is a founder and director of Hitwise."

- *Heavyweights back Sinewave*[9], by Jane Schulze, The Age (Business, p5), 13 Jul 2000:
  "...Mr Barlow said Hitwise differed from competitors by measuring traffic passing through about 45 local Internet service providers ... 'Our product is plug−in−and−play, highly transportable and very scaleable,' he said. ..."

28. Individuals with a basic understanding of how the Internet works would know that market analysts/researchers cannot know how many individual visits are made to any particular web page, nor where they were visiting before or after, without access to the IP address of the computer used by the Internet user.

29. Many users would also know that the IP address can be used to identify some individuals.

30. Concerned individuals, on visiting the Hitwise website, would have found it readily apparent that Hitwise uses IP addresses which are made available to Hitwise by some ISPs, which Hitwise refers to as "partners". For example:

- *"The Hitwise service provides [Hitwise's] clients with an indication of the relative popularity of websites, based on the measurement of visits, visit duration or page downloads from a range of geographically diverse ISP networks. The [ISP] proxy server records requests for web pages made by the ISP's users. Hitwise then analyses these proxy server records daily, to produce website rankings across more than 150 subject categories."*
  ("About Hitwise Australia" page, as at 16 Dec 2004[10])

- *"Most IP addresses analysed by Hitwise are unique to an individual and are not serving more than one visitor.*

...
Hitwise has developed proprietary software that can analyse a range of usage logs from ISPs or via the opt−in mega panel. These usage logs can be created in three unique ways.
1. Via proprietary client based tracking systems, or
2. Via proxy servers, or
3. Via Hitwise's proprietary 'packet sniffing' hardware technology that extracts the usage data directly from an ISPs network creating a real−time log of all user activity. ..."
(Hitwise Methodology FAQ, as at 2 Dec 2004[11])

31. Visitors to the Hitwise website would also be given the understanding that the *Privacy Act 1988* does not protect them from having their online activities monitored and/or tracked by Hitwise, nor prevent Hitwise from disclosing information about them to other organisations:

Hitwise Privacy Statement, as at 16 Dec 2004[12]:
"...Legal nature of this Privacy Statement
"...Hitwise will act to ensure it complies with the privacy principles contained in this statement, but is not legally bound to enforce these principles under Australian law."

32. Some individuals may conclude from the above that Hitwise is a small business exempt from compliance with the PA, while others who have read media reports stating that Hitwise had a turnover of $20 million in 2004 (Herald Sun, 19 July 2004 [13]) may wonder whether or not Hitwise is required to comply with the PA.

33. We consider it highly unlikely that community trust in Internet businesses, and confidence that privacy "rights" are being protected, will increase while personal information about individuals continues to be disclosed and collected in ways such as the above without the prior express consent of the subject individuals. Collecting IP addresses capable of identifying individuals and details of sites visited not only invades individuals' fundamental right to privacy, but would also enable the compilation of detailed profiles about individuals that can make them susceptible to discriminatory business practices such as redlining/weblining as discussed later herein.

34. Furthermore, it appears to us that the above disclosure and collection practices would be in breach of one or more existing Commonwealth privacy protection laws. However, if that is the case, then it appears that some ISPs and Hitwise are not aware of existing laws or choose to thumb their noses at same due to lack of enforcement. Apparently relevant laws are:

Telecommunications (Interception) Act 1979

Use of "'packet sniffing' hardware technology that extracts the usage data directly from an ISPs network creating a real−time log of all user activity" would involve interception (recording) of highly transitory communications during their passage over the telecommunications network. Such interception is in breach of the *Telecommunications (Interception) Act 1979*[14] ("TIA") unless it is done by a law enforcement agency that has obtained a telecommunications interception warrant. (Other exemptions in the TIA are not relevant to this scenario).

According to an article in the Sydney Morning Herald (*Web stats firm in flap over 'packet sniffing'*[15]) on 10 December 2004, Hitwise said "claims on its own website that it used potentially illegal packet−sniffing hardware to harvest information was a mistake".

However, the technical information in Hitwise's patent application for a "Method And System For Characterization Of Online Behavior"[16] leaves open to serious question whether or not the system is in fact real time packet sniffing technology. At the very least, the system cannot operate as claimed in the patent application without access to the IP addresses of individual Internet users and IP address can be used to identify individuals.

Telecommunications Act 1997

Whether or not the system involves 'packet sniffing' in breach of the Telecommunications Interception Act 1979, disclosure of the information by ISPs appears to be in breach of the *Telecommunications Act 1997* ("TA"). Part 13 ("Protection of Communications") of the TA prohibits ISPs from using or disclosing any information that (among other things) relates to the affairs or personal particulars of telecommunications users and the contents of communications that have been, or are being, carried by carriers or carriage service providers including ISPs (s276). While the TA contains some exemptions to the s276 prohibition, none of these would apply to the disclosure of information about Internet users and their communications by ISPs to Hitwise, that is, to an entity that is not a law enforcement agency and is not another carriage service provider.

Privacy Act 1988

If relevant ISPs argue that neither the TIA or TA is applicable to the information they disclose to Hitwise (an argument that EFA considers most unlikely to be persuasive to a court), then the Privacy Act 1988 ("PA") would be applicable.

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" (or has consented). Given IP addresses can be used to identify some individuals and Hitwise states that "[m]ost IP addresses analysed by Hitwise are unique to an individual and are not serving more than one visitor", it seems clear that some of the information being disclosed by some ISPs to Hitwise is personal information protected by the PA.

EFA considers it is highly doubtful that a secondary purpose of using and disclosing information (collected for the primary purpose of providing a carriage/Internet access service) to Hitwise to enable Hitwise to sell market analysis and research services to third party businesses can be seen to be **related** secondary purpose within the meaning of the PA. However, even if it could be, the second part of the NPP 2.1(a) test is not met. The vast majority of individuals would not reasonably expect their ISP to be disclosing information about them and web pages they visit to an organisation such as Hitwise. Even if some individuals would expect same or have consented, the indiscriminate bulk nature of the disclosures by ISPs to Hitwise would result in breach of NPP 2.1 in relation to individuals who do not expect their information to be used and disclosed for such a purpose and have not consented.

With regard to the collection by Hitwise from ISPs, this scenario also demonstrates a concerning loophole in the Privacy Act 1988. There is no restriction on organisations collecting information about individuals for their own *primary* purpose from a third party and using and/or disclosing the information for that primary purpose, without the subject individual's knowledge and consent, including when the individual would not even

reasonably expect same. More detailed information in this regard is provided in the section *Primary and Secondary Purposes of Collection* later herein.

35. If the collection and disclosure activities referred to above are not currently prohibited by Australian law, then in our view the law needs to be changed. On the other hand, if ISPs are currently prohibited from using and/or disclosing the information without consent, or Hitwise is prohibited from collecting and/or using the information without consent, the most effective and appropriate means of increasing community confidence would be for regulators to enforce the law. However some regulators decline to enforce the law, an example of which is provided below.

(b) Disclosure of silent and other blocked calling numbers

36. As mentioned earlier herein, several events associated with the commencement of the *Privacy Amendment (Private Sector) Act 2000* have resulted in individuals having less privacy rights than previously. .

37. For example, since 21 December 2001 when the private sector provisions commenced and the telecommunications industry privacy protection code was de−registered, Telstra and some other telephone call carriers have commenced disclosing silent and other blocked calling numbers to the end recipient of telephone calls, in particular, to dial−up Internet Access Providers.

38. A representative complaint was made to the regulator, the Australian Communications Authority[17], in July 2003. Over twelve months later, in August 2004, the ACA communicated its findings and decision to the three complainants (one of whom is also EFA's Executive Director). The ACA said it had found that some telephone call carriage service providers (at least Telstra, Comindico and Optus) are illegally disclosing silent and other blocked calling number information to some ISPs as alleged in the complaint. The disclosures are in breach of s276 of the *Telecommunications Act 1997*, an offence which carries a penalty of imprisonment.

39. However, the ACA decided not to take any action to prosecute the offences, nor even direct the offenders to comply with s276 of the Act from then on.

40. EFA questions what point there is in Parliament enacting legislation while regulators empowered to enforce the law refuse to do so.

41. The ACA subsequently issued a misleading media release, titled *"ACA issues warning on silent and blocked numbers*[18], on 26 August 2004. It stated:

> "*People with unlisted numbers, or those who have blocked calling number display, need to be careful about letting another person use their phone line to access the Internet, the Australian Communications Authority (ACA) warned today.*
> *'Letting another person use such a phone line to access the Internet could lead to the number being disclosed to and used by that person's Internet service provider,' ACA Acting Chairman Dr Bob Horton said. ...*"

42. The ACA media release failed to mention the fact that the only reason people need to "be careful" is because telephone call carriers are breaching the law and the ACA has declined to enforce the law.

43. Furthermore, we believe there are far more illegal disclosures occurring and in a significantly wider range of circumstances than was determined by the ACA. The ACA was of the opinion that many disclosures were permitted by the s291 exemption to the s276 offence. However, we believe the ACA's opinion is wrong because among other things their analysis failed to take into account the fourth element (clause (1)(d)) of the s291 exemption to the s276 offence, which must be satisfied for that exemption to apply. Failure to take the fourth element into account results in a conclusion that some disclosures are lawful in circumstances in which they are not lawful. In addition, we consider the ACA's construction of the law in relation to the "former" customer component of s291 is arguably incorrect.

44. If the ACA's interpretation of the law is correct, then the s291 exemption authorises businesses in the telecommunications sector to use and disclose many other types of personal information (not only silent and blocked calling numbers) for purposes which we believe the Government and the Parliament did not intend and for which many individuals would not consent nor even reasonably expect. These include:

- use and disclose personal information without the subject individual even being "made aware" including:
  - ♦ use and disclose personal information about individuals who are **former** customers of the disclosing business, including when that business has collected the personal information from a third party many years **after** the individual ceased to be a customer of that business
  - ♦ disclose personal information about individuals who are not customers of the business to which it is disclosed and who have no wish to become a customer of that business (e.g. disclosure to another business for the recipient business's direct marketing purposes)
  - ♦ disclose personal information that is **not** necessary for one of the recipient business's functions or activities. According to the ACA's decision, the s291 exemption does not involve a needs test notwithstanding that the intent of the exemption is plain in the section title *Business needs of other carriers or service providers*.

45. Irrespective of the correct interpretation, it is fact that some telecommunications service providers are relying on s291 to use and disclose personal information in circumstances that would otherwise be in breach of NPP 2 and that are very unlikely to have been intended by the Parliament in enacting s291 of the TA. Such use and disclosure is also contrary to previous interpretations of s291 made publicly available by the ACA and TIO, for example:

- Previously ACA registered ACIF Industry Code−*Protection of Personal Information of Customers of Telecommunications Providers*[19] (p18)
  "...section 291 of the Act...allows uses for the business needs of other carriers or service providers (which would generally be accompanied by a disclosure...) that are associated with providing a service **to the person who is the subject of the information or document**. This provision is designed to allow uses/disclosures which are 'triggered' by some action or request by a customer such as dialling an access Code to make use of another carrier." (emphasis added)

  (Notably, in relation to the complaint referred to earlier herein, Telstra commenced disclosing personal information in circumstances other than the above three months after the Code was de−registered. The relevant Telstra service had operated without such disclosures for the previous 18 months, i.e. since November 2000, at which time the Code was

registered. Obviously it was not (and it still is not) technologically necessary to the ISPs' operations for Telstra to disclose the personal information.)

- ACA Telecommunications and Law Enforcement Manual[20]
  "to permit a carriage service intermediary to pass on the details of a customer to a network operator so as to permit connection. Disclosures would also be permitted where a customer changes his or her CSP."

- TIO Position Statement, 2003[21]
  to allow a "provider who has the customer's details to disclose the customer's information to another provider [e.g. a 190 calls provider] so that it can bill for the calls made"

46. In our view, either the PA or TA must be amended so that *all* businesses in the telecommunications services industry are required to comply with NPP 1 in relation to *necessary* collection and NPP 2 in relation to use and disclosure, so that TA s291 (and the related s302 secondary use/disclosure exemptions) cannot be interpreted or applied in a way that authorises breach of NPP 2 of the PA. Compliance with those NPPs would not prevent service providers collecting, using and disclosing information for necessary purposes such as those stated by the ACA and TIO above.

47. A complaint was also sent to the Federal Privacy Commissioner in July 2003 (at the same time as to the ACA) alleging breaches of *Privacy Act 1988* (which covers some matters on which the *Telecommunications Act 1997* is silent). Eighteen months after lodging the complaint, the complainants are still awaiting a decision by the Commissioner.

(c) Integrated Public Number Database ("IPND")

48. Another example of the inadequacy of existing privacy protection legislation is the mis−use of personal information that is legislatively required to be recorded in the Integrated Public Number Database ("IPND").

49. In March 2004, the Australian Communications Authority publicly announced that its investigations had revealed that telecommunications "customer information was being used for purposes beyond those specified or contemplated within Part 13 of the Telecommunications Act" and that "the IPND [Industry] Code was failing to properly regulate the use of customer information". The ACA also said that it had therefore "decided to determine a mandatory industry standard to regulate the use of telecommunications customer information".

50. The ACA advised in early December 2004 that it was intending to issue a draft industry standard for public consultation in January 2005. However, it has still not been released.

51. While EFA recognises there are complex issues involved in developing an appropriately balanced industry standard, we are disturbed that the mis−use of customer personal information has been allowed to continue for over 15 months since the ACA decided (in November 2003) that an industry standard was necessary.

52. Further information about the IPND issue is available in EFA's submission to the Australian Communications Authority[22] and the ACA's discussion paper titled *Who's Got Your Number?: Regulating the Use of Telecommunications Customer Information*[23].

(d) Email, SMS and Voice Mail

53. The advent of new telecommunications technologies in the form of email, SMS and voice mail services has resulted in individuals having less legislated privacy rights when using these technologies than when they communicate by fax or a normal telephone call. Recent changes to the *Telecommunications (Interception) Act 1979* ("TI Act") allow email, SMS and voice mail to be lawfully intercepted during transit in circumstances that were previously illegal, including by staff of telecommunications service providers.

54. Such broad all encompassing changes to the law were not necessary to achieve the claimed objective of the amendments to the TI Act and should be repealed.

55. The above issue is discussed in detail in EFA's submission to the Inquiry into the Provisions of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*[24] conducted by the Senate Legal & Constitutional Legislation Committee.

▲ Go to Contents List

4.2 Computer Technology in general

4.2.1 Private enterprise searches of computers

56. Relatively new technologies enabling a "vacuum cleaner" approach to searches of computers have given rise to serious privacy issues in connection with search warrants and court discovery orders. In particular, the protection of the rights of not only a suspect, but also third parties, in relation to matters of privilege, confidentiality and privacy. Issues are arising in relation to seizure of information from computers not only in relation to search and seizure of, for example, Senators' computers by police[25], but also during search and seizure raids by civil litigants who have obtained an Anton Piller order made by the Federal Court and other courts.

57. Although Anton Piller orders have been used for many years by business interests in Australia, few members of the general public had heard of them before 2003/2004 when they hit the headlines following music industry raids at universities, Internet Service Providers and people's homes.

58. The Australian Law Reform Commission ("ALRC") discussed the matter of Anton Piller orders in an ALRC Report[26] issued in 1995. Among other things the ALRC said "Is there cause for concern?" and then remarked that "[t]here is widespread international concern about the execution of Anton Piller orders".

59. While there was cause for concern in 1995, since then the law relating to Anton Piller orders in Australia has been extended by Courts in ways which have "greatly increased the scope and effect" of Anton Piller orders[27].

60. In EFA's opinion, the extension of the law since 1996 suggests that there is now cause for alarm. EFA is extremely concerned that the novel applications for Anton Piller orders that the Court has been faced with in 2003/2004[28] and the practices of the courts to date appear to have high potential to result in inappropriate and unnecessary invasion of the privacy of third and fourth parties, that is, of law−abiding members of the public.

61. A number of raids conducted by civil litigants under Anton Piller orders in 2003 and 2004 at homes, universities and Internet Service Providers have resulted in increased public concern, in part because orders made by the Federal Court have included authorising copying of information from computers owned by third parties, including entire hard−drives. For example, an Anton Piller order made by the Federal Court in February 2004 permitted the applicants to enter the homes and premises of third parties including universities and Internet Service Providers and seize electronic materials including "information recording communications" by way of making "bitstream images". The making of a "bitstream image" is a computer forensic process used to make a copy of the entire hard drive of a computer. It is what has been referred to as the "vacuum cleaner" approach to search and seizure.

62. Furthermore, some orders have knowingly authorised invasion of the privacy of third parties without adequate safeguards and controls. For example, in the Federal Court case of *Sony v University of Tasmania* [2003] FCA 532[29], the court "in effect condoned a large scale fishing expedition through an intermediary's records"[30]. The intermediary in question was a University providing computer network services and the litigants gained access to computer backup media that "contained home directories, web spaces, email spools and any other data stored on the relevant servers"[31], thereby invading the privacy of many innocent and uninvolved third parties. This access to personal information was recognised by the judge, who said that the accessed material "will include a great deal of extraneous and irrelevant material" including material "which may be privileged or subject to confidentiality obligations"[32]. The only protection afforded to the privacy of those third parties was an undertaking by the applicant's solicitors not to mis−use that information; however, as has argued elsewhere "once private information about an individual has been disclosed, his or her privacy is already infringed"[33]. Also, "mis−use" of that information is an ambiguous concept and in EFA's view much stronger privacy protections are required.

63. According to the Federal Court's web site as at 25 January 2005, the Practice Notes concerning Anton Piller orders[34] have not been changed since first issued in 1994. In view of the Court's recent practices in issuing orders authorising "vacuum cleaner" approaches to computer searches, it appears there may be a need to amend the *Federal Court Act 1976* to regulate the Courts' powers in this regard, and/or specifically require the Court to develop additional Rules and/or Practice Notes concerning search and seizure of computers and information contained in computers, to ensure appropriate protection of the privacy of third parties when information is indiscriminately seized via a "vacuum cleaner" search.

64. More detailed information about this issue is available in Section 9 of EFA's submission to the Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation[35] currently being conducted by the Senate Standing Committee for the Scrutiny of Bills.

4.2.2 Spam & Unnecessary Search Powers

65. While the emergence of spam led to legislative prohibition on the sending of some types of spam (*Spam Act 2003*), at the same time the Parliament passed legislation granting some government agency employees, not only police, the right to invade the privacy of the homes and other premises of **victims** of spammers, that is, of recipients of spam.

66. Such broad search powers were not necessary to achieve the objective of the legislation and should be repealed. The relevant amendments to the Bill passed by the Senate, but subsequently not insisted upon, should be enacted.

67. The above issue is discussed in detail in Section 3 of EFA's submission to the Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation[36] currently being conducted by the Senate Standing Committee for the Scrutiny of Bills. It was also raised in EFA's submission to the Inquiry into the *Spam Bill 2003* and *Spam (Consequential Amendments) Bill 2003*[37] conducted by the Senate Environment, Communications, Information Technology and the Arts Legislation Committee.

▲ Go to Contents List

4.3 'Smart Card' technology and the potential for use to establish a national identification regime

4.3.1 The Road to an *Australia Card*

68. EFA considers the roll out of smart cards by government has an extremely high potential to result in the equivalent of an Australia Card[38], whether or not that is the government's intention at the outset. This potential arises from a combination of factors including the ease with which smart cards can be used for two−way communication with a centralised database and that smart card technology is designed to facilitate function creep.

69. Although smart cards are often referred to as being new technology, they are not new. Smart cards were invented in Europe over 30 years ago and since then have been largely a solution looking for a problem. In 1990/91, the Health Insurance Commission ("HIC") issued tender documents seeking provision, among other things, of smart cards and related card readers. Following public fears that the government was intending to turn the Medicare card into an Australia Card by stealth (the then recently defeated Australia Card would have been administered by HIC), the then Minister for Health stated[39] the Government had no intention of introducing a Medicare smart card.

70. Currently smart card technology is being touted as the solution to many identity management and other issues. However, there is little if any indication of adequate attention being given to the serious security and privacy risks inherent in use of smart card technology and whether or not use of the technology would solve the claimed problems and/or would also introduce new problems.

71. Consequently, EFA is highly concerned by the proliferation of proposals by governments and government agencies to foist use of smart cards on a largely unsuspecting public. In Australia, these include:

- the Commonwealth government's Medicare smart card (and proposed HealthConnect centralised database);
- the Queensland Government's proposed multi−function Driver Licence smart card (which we understand other States/Territories are watching with a view to similar inter−operable implementations);
- reports that the Commonwealth Government is considering the use of smart cards to control use of welfare payments by recipients.

72. Even if a smart card is rolled out as single use/purpose, or "voluntary", together with legislative and technological controls to prevent function creep, history demonstrates that such controls are likely to be over−ridden by government in the not very distant future.

73. An excellent example of function creep is the Tax File Number ("TFN") which was introduced following the defeat of the Australia Card. As pointed out by former Federal Privacy Commissioner, Malcolm Crompton, in his March 2004 speech *Proof of ID required? Getting Identity Management Right*[40]:

> *"...TFNs are designed primarily to collect together the taxation−related information about each individual. There is a Voluntary Quotation Principle (Guideline 1.2 of the Tax File Number Guidelines), by which quoting one's tax file number is guaranteed to be voluntary. However, individuals who do not quote their TFN to employers and financial institutions have tax deducted from their income or interest payments at the highest marginal rate plus the Medicare levy.*
>
> *When the Tax File Numbers first came into effect in 1988, for many people, the only penalty for not quoting it was that for some income, for example a dividend stream, you made an interest free loan for less than a year to the Tax Office of the difference between the top marginal tax rate and the marginal tax rate you paid (this amounted to nothing for high income earners and not much for most others).*
>
> *Through a range of legislative changes since 1988, it is now the case that some Australians are not able to survive without obtaining and quoting their TFN (for example, to obtain unemployment benefits and a number of other interactions with Government). But the Voluntary Quotation Principle is still in place: if you are unemployed, you do not have to receive unemployment benefits, so you do not have to quote your TFN!*
>
> *The function of the Tax File Number has moved from, as it was initially, a purely taxation−related function, to the present situation, where it is used to cross match data relating to government assistance of various sorts and superannuation.*
>
> *Not only is the TFN story a good example of function creep, it also illustrates how privacy promises made in law can be lost over a very short period of time."*

74. The probability of function creep with a smart card is far greater than what has occurred with simply a number. This could occur, for example, in the form of:

- additional government mandated uses of the same smart card;
- additional mandatory personal information (text and/or biometric data) being loaded onto the smart chip;
- additional applications being loaded onto the smart chip;
- smart card readers berg linked to one or more centralised databases;
- increased government agency and business insistence on "voluntary" presentation of the smart card as a condition of provision of goods and services because a smart card may be regarded as strong evidence of identity (regardless of whether it is or not) and because the card is computer readable and so enables automated capture of data from the card by the agency or business.

75. The smart card industry makes no secret of the fact that smart card technology itself facilitates function creep and some, perhaps all, suppliers are readily able to explain to governments how they could roll out an Australia Card equivalent to a largely unsuspecting public by stealth. SchlumbergerSema, for example, said in their January 2003 submission to the UK Home Office[41]:

"Getting there − An iterative process

The well understood sensitivity of the [ID card] issue indicates the need to progress gradually rather than by 'big bang'. Because of the history and tradition of the British people, we believe that arriving at a universal entitlement [ID] multi−application smart card may be an iterative process stretching over a number of years.
...
We believe that trying to move from where we are now to a sophisticated smart card solution without one of these interim steps would underestimate the business process and social attitude changes that would need to take place".

76. SchlumbergerSema therefore suggested either of two paths, comprising a smart card containing minimal information, from which it would be possible to migrate "*to the sophisticated smart card at a later date, once the concerns over entitlement [ID] cards have been addressed*".

77. An iterative process was also recommended in a June 2002 report prepared for VicRoads[42] which, in effect, sets out a blue print for an Australia Card equivalent. The authors state:

"*Since the proposed Australia Card in 1986/87 [sic] the development of smartcard technology in Australia has lagged behind may other countries, including much of Asia.*
It is now recognised that the Australia Card experience delayed the introduction of smartcards by some ten years."

78. The report notes that a multiple application smartcard driver licence "*may be perceived by some as a latter day 'Australia Card'*" and "*has technology, project and privacy risks, but these can be addressed by: ... phased introduction, i.e. start with the basic driver licence and gradually expand as customers become ready*". Among other things, a key aim of the study was to "*adopt a simple solution initially but build in capacity to expand to multiple applications as users become ready to accept new applications*" (emphasis in original).

79. EFA considers it is extremely unlikely that the many Australians who opposed the Australia Card and those holding similar views about their privacy now would ever "be ready" to accept the future "new applications" proposed in the VicRoads report. These included health/medical data, other licences (business, marine, fishing, wildlife and game, firearms), whole of life events, electronic voting, public transport ticketing, road tolling, parking, bank credit card (co−branded with driver licence), etc.

80. However, as SchlumbergerSema pointed out in the submission previously mentioned "*once people have smart cards in their hands, those cards and the chips on the cards are easy to upgrade...*".

81. Furthermore, once smart cards and card readers are in wide use, there is no technical impediment to linking card readers to centralised databases run by either government or business which records all interactions with government agencies and/or businesses together with identity and location information. For example, as the VicRoads report pointed out:

"Smart card interoperability can incorporate ... driver licence card utilizing the EFTPOS network and a government concession network".

82. Moreover, the risk of function creep in relation to a unique identification number connected with a newly issued smart card, such as the Medicare smart card, is significantly greater than with existing numbers issued by the Commonwealth Government. The existing Medicare numbers and Tax File Numbers cannot be regarded as necessarily a unique identifier nor adequate evidence of identity because the related databases recording to whom a number was issued have long been known to be corrupt.

83. In the case of the existing Medicare numbers, these were rolled out in a rush during 1984 and as noted in the Auditor−General's 2004−05 audit report on the integrity of Medicare enrolment data[43]:

> *The net result was that, by the end of the 1984 enrolment period, the HIC database had been corrupted, but to an extent that was never, and has never been measured.*

84. In the case of TFNs, as reported by the Standing Committee on Economics, Finance and Public Administration in *Numbers on the Run*[44]:

> *The ANAO found that there were '3.2 million more individual TFN registrations than people in Australia counted in the last census'. In further reviewing this issue, the ATO identified 5.3 million potentially inactive (ie excess) registrations on the ATO individuals data base.*

85. In view of the known problems with existing databases, the rollout of the proposed new Medicare smartcard and associated numbers (both Medicare and HealthConnect numbers) seems likely to be undertaken in a manner that would avoid the same problems. The staged rollout (rather than the rushed rollout that occurred in 1984), together with the requirement that existing Medicare card registrants provide 100 points proof of identity (the same as when opening a bank account), would result in unique and reliable national identification numbers for the first time in Australia.

86. As a result the smart card itself seems likely to become requested, or required, as a *primary* proof of identity document, unlike the existing Medicare card which is used as a secondary document. Whether this will occur will depend in part on whether a card's chip contains the "optional" photograph/s and of course whether inclusion of photograph/s remains optional.

87. The design of the Medicare smart card itself also raises questions as to whether it has dual purposes, one being the gradual rollout of an Australia Card by stealth. The commonly promoted security features of smart cards are apparently not the reason for use in this implementation as those features are not being used. According to the "privacy information" issued by HIC[45]:

> *All information stored on a Medicare smartcard can be accessed by anyone who is in possession of the card and a card reader, including situations where the card has been lost or stolen.*

88. Photographs will be stored on the chip on the smart card, not printed on the face of the card. Therefore to compare the individual presenting the card with a photograph, it will be necessary to place the card in a card reader. Once a card is placed in the reader, the business or agency would be able to automatically and covertly capture and record all information stored on the card chip in its own computer database and/or covertly transfer the information to another organisation or agency's centralised database.

89. Hence the card has a high potential for use as a surveillance device to track and record individuals' interactions with government agencies and businesses.

90. We share the views expressed by AMA President, Dr Bill Glasson[46], that this particular smart card

> "*is not such a smart idea ... a genuinely useful Smartcard [would] securely protect[s] the privacy of patients' health information.*
> *A really smart Smartcard would only be used for specific health purposes and could not be linked to other personal information.*
> *A really smart Smartcard would be the product of consultation and agreement between Governments, patients, consumer groups and the medical profession.*"

91. We have been unable to ascertain why a smart card is being used other than vague statements that people "may" at some time in the future be able to record details of allergies on this insecure card. Furthermore, apparently no privacy or security impact assessment was undertaken prior to commencing to issue Medicare smart cards.

92. In view of the above, the Medicare smart card has all the hallmarks of an iterative process leading to the Australia Card Mark II. Such a process would involve telling an unsuspecting public, many of whom know little about technology, they need a new "smart" card without justifying why and require them to submit 100 points proof of identity. It would also involve telling them that the card and the photograph are optional in the hope that a significant majority of the population will opt−in. The next stage would occur in a few years when the remaining members of the public who had declined to opt in would be told that it has become too costly, or impractical, to continue with two different cards so the smart card and reliable national identification number has become mandatory. Thereafter it is a relatively simple matter to add new applications to the card, as just one example, to control the type of purchases that may be made with welfare payments.

93. As the national president of the Australian Computer Society, Edward Mandla, remarked recently in The Australian[47]:

> *There have been suggestions in recent months that the new Medicare SmartCard associated with the Commonwealth HealthConnect program could be an Australia Card by stealth, because it includes an embedded microchip with a range of functionality, including the ability to store health data and a unique patient identification (UPI) number.*
>
> *It is essential that all potential uses for this number are defined and made public, including what type of data can be linked to the card, who will have access and how it can be used.*
>
> *The intense opposition to the original Australia Card proposal was partly the result of concern about function creep, because of a lack of detailed definition over the storage and use of personal data.*
>
> *If there is any suggestion of a national ID system being introduced in Australia, it must be debated vigorously in the public arena before any decisions are made.*

94. If the Medicare smart card and/or the Medicare or HealthConnect identification numbers are not intended to be the Australia Card Mark II, the rollout of the Medicare smart card should be halted while an independent privacy impact assessment and a security impact assessment are undertaken, the resultant reports made publicly available and identified issues addressed after public consultation.

95. Furthermore, at the very least, security measures should be built into the smart card designed to prevent access to the information on the chip without the informed consent of the card holder and legislation (not disallowable instruments) needs to be enacted that:

- aims to ensure the smart cards and photographs will remain genuinely optional; and
- makes it a serious offence for Commonwealth, State and Territory government departments/agencies and businesses (and their staff) to discriminate against any person who declines to possess, or declines to present, a Medicare smart card as evidence of identity or for any other purpose; and
- prohibits collection, use and disclosure of the Medicare and the HealthConnect numbers by government agencies and businesses unless the prior express consent of the relevant individual has been obtained, or the relevant government agency or non−government health sector purpose is *specifically* authorised by legislation; and
- prohibits storage of copies or originals of the photographs in an HIC or any other government or business database or other storage facility.

96. Meanwhile in the absence of (at least) all the above (which may well be forever), Australians concerned about their privacy and the potential for Big Brothers and businesses to encroach further into their daily lives would be best advised to decline the government's "offer" of the Medicare not−so−smart card. In addition, Australians who want a smart health care card may also be best advised to reject the not−so−smart card currently on offer as it appears mass rejection of the current card may be the only means by which a genuinely smart health card may eventuate.

97. Similar issues and problems exist with the Queensland Government's proposed multi−purpose Driver Licence smart card. Detailed information is available in EFA's submission to Queensland Transport re Smart Card Driver Licence Proposal[48].

4.3.2 Technological Security Issues

98. EFA is also highly concerned that the public is being told that smart card technology in general is extremely secure despite evidence to the contrary. For example, the Queensland Government is intending to implement a Smart Card Driver Licence and the public has been told that:

> *Smartcard technology allows information to be stored on the computer chip or "smartchip". The technology is well tested, reliable, and meets rigorous security and integrity standards.* (Qld Transport's Smart Card Driver Licence Project Snapshot leaflet[49])

> *Any attempt to crack the 'keys' of this type of smart card technology would be extremely expensive. A would−be hacker would need to invest in several millions of dollars in technology just to crack one card... The layers of security available with smart card technology will ensure licence holders can be confident that their information is extremely secure.* (Attachment to Qld Minister for Transport's media release dated 29 Sep 2003)

99. The above statements misrepresent the facts concerning security of smart cards. While smart cards may be tamper−resistant, they are not tamper−proof.

100. Methods by which the claimed security of smartchips can be breached, without investing in expensive technology, had previously been publicised including recently discovered new methods. As stated in the VicRoads report, the risks of using a smart card for a driver licence (or for that matter anything else) include *"a potential major security breach, e.g. hacking, emulation, differential power analysis"*. Indeed, it was subsequently reported that a differential power analysis attack was successfully undertaken by a Sydney university student (see later herein).

101. Given the costs and issues involved in overcoming recently discovered security flaws, it is likely such flaws exist in some, perhaps many, chips currently being sold. Furthermore, reportedly at the DATE 2004 conference in Paris last year[50], smart card designers were clamoring for security tools to evaluate chips at the design level for possible leakage of confidential information.

> *"The lack of tools to combat threats and tampering on smart cards is ... looming as a big concern for smart card designers. Laurent Sourgen, director, product development, smartcard division, at STMicroelectronics, said, 'There are no universal tools' optimized for meeting such critical challenges faced by smart card designers."*

102. Further, the assumption apparent in the Qld Transport documents that the cost of cracking a security device is relevant to the adequacy of protection of information on a smartcard is incorrect. This is because the expenditure necessary depends on the timeliness of the protected data. For example, although it might take several million dollars of technology to crack a security device in less than one day, it may take only a few thousand dollars to crack it in six months. If the data is still valuable in six months' time (e.g. individuals' identity information), then it does not matter if it takes six months to crack it.

103. Information on known security flaws is freely available, for example, see:

- Smart cards also open to attack[51], Australian IT, 19 November 2002
  "Sydney University engineering student Ryan Junee has demonstrated a smart card attack for his final year thesis, using a method called 'differential power analysis'. Using software he developed and a cathode ray oscilloscope (CRO), Mr Junee showed that cards using Data Encryption Standard (DES), or even triple−DES, could be interrogated to reveal secret information such as keys and PINs."
  - Thesis, "Power Analysis Attacks :: A Weakness in Cryptographic Smart Cards and Microprocessors"[52], Ryan Junee, November 2002
  - Smart Cards and Side−Channel Cryptanalysis[53], Ryan Junee, Ruxcon Security Conference, Sydney, April 2003
- On a New Way to Read Data from Memory[54], David Samyde, Sergei Skorobogatov, Ross Anderson and Jean−Jacques Quisquater, First International IEEE Security in Storage Workshop, USA, 11 December 2002
  "This paper explains a new family of techniques to extract data from semiconductor memory, without using the read−out circuitry provided for the purpose. ... The goal of this work was to explore new ways of recovering data directly from the memory of smartcards and other security processors without using the read operations provided by their vendors for that purpose, thereby circumventing any access controls and reading out secret data directly."

- Camera flash opens up smart cards[55], New Scientist, 13 May 2002
  "Sensitive information stored on a smart card microprocessor can be revealed with a flash of light, say UK researchers.
  Sergei Skorobogatov and Ross Anderson of Cambridge University have discovered that firing light from an ordinary camera flash at parts of a smart card microchip can assist an attacker in determining the sensitive information stored on the card. This might include, for example, the cryptographic key used to gain access to a building or to secure internet transactions."
- Lasers crack the key to smartcard chip secrets[56], EE Times, 20 May 2002
  "Dr Anderson said: 'Sergei's work will trigger a generation change in smartcard technology. The immediate effect of his work is that many attacks on computer systems that were developed as theoretical possibilities by the research communities in the 1990s have suddenly become practical.'"

- Smart Card Security − Defining 'tamperproof' for portable smart media[57], Stefano Zanero, Dipartimento di Elettronica e Informazione, Politecnico di Milano, 2001
- Tamper Resistance − a Cautionary Note[58], Ross Anderson & Markus Kuhn, Cambridge University Computer Laboratory

104. We are also disturbed by the attempts to undermine and/or ignore legitimate concerns by claiming that concern arises from ignorance about the technology. For example, the Qld Transport 'Privacy Information Paper' (page 10)) states:

> *There are perception risks about chip technology such as remote and secret reading or scanning of information. Demonstrations of the new licence and its operations, public education campaigns, security features and legislative and contractual protections will be used to address these issues.*

105. However, they are not "perception risks", they are actual risks. Moreover, it is largely irrelevant whether or not information is read secretly. The issue is whether a smart card holder voluntarily consents to use and disclosure of their personal information and the high risk that government mandated use of smart cards will result in the equivalent of an Australia Card.

▲ Go to Contents List

4.4 RFID / Microchips

106. EFA is highly concerned by the lack of legislative controls on use of radio frequency identification chips (RFID, Contactless Integrated Circuits, etc) not only in relation to implantation in human beings, but also implantation into documents that individuals are required to carry and into clothing and other consumer goods.

107. EFA is a signatory to the international *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*[59].

108. We consider the *Australian Passports Act 2005* to be a good example of the dangers of RFID technologies. We find it astounding that the legislature has passed vague legislation granting a Minister broad powers to force individuals to carry radio frequency surveillance devices containing unspecified biometric data. As stated in the relevant Bills Digest, No. 75 2004–05[60]:

"...clause 47 provides that the Minister may determine particular methods and technologies that are to be used to confirm 'the validity of evidence of the identity' of an applicant for an Australian travel document...

The Minister has said that the Australian Passports Bill 'provides for the introduction of facial biometric technology as an effective means of verifying identity'. While the use of such technology may lie behind the inclusion of clause 47, biometric technology (howsoever described) is not mentioned at all in the Bill. The Explanatory Memorandum suggests that the phrase 'methods (and technologies)' in clause 47 could include 'facial biometrics' (being measurements of a person's face that can allow a computer to verify the identity of a person). However, given the breadth of the language used in clause 47 (or rather, the lack of any specificity as to what method or technology might be used), the phrase could also include fingerprinting or the use of genetic information (such as DNA testing and comparison).

In terms of biometrics (which includes facial recognition, fingerprinting and iris scanning), 'the validity of evidence of the identity' of a person could be confirmed by two means: Machine Readable Travel Documents (MRTDs) and a database of biometric details."

109. In short, the Minister has been given the power to determine, for example, that DNA must be collected from passport applicants and the DNA profile stored in a government database accessible by overseas government agencies. There is no conceivable reason for the granting of such broad powers, especially given that by February 2004 the International Civil Aviation Organization ("ICAO") had adopted facial recognition as the global standard for biometric identifiers in passports and a biometrics database is not required to comply with international standards.

110. The particular type of computer chip to be implanted in passports is also a danger to individuals' security and privacy. While these chips are often referred to as "RFID", they are actually radio frequency "Contactless Integrated Circuits"[61]. The difference is that true RFIDs contain very little data storage space and therefore can broadcast only, for example, an identification number, while the passport chips can store and broadcast significantly more personal information including a photograph, which could be used from a distance to identify and track individuals without their knowledge or consent[62]. The chips that the Sharp Corporation has said it is supplying[63] for the Australian Government's e−passport pilot program incorporate 512 kbyte flash memory. This capacity is large enough to hold not only the facial photograph required by the ICAO−defined standard, but also finger−and iris−prints.

111. The information on the chips can be read remotely by anyone with any reader, not just by the reader to be used by immigration/customs officials. Furthermore, as reported in the Electronic Engineering Times[64], tests of electronic−passport interoperability have exposed technology flaws and:

"...it was intrusion, not precision, that was on the minds of the security experts and privacy advocates who expressed alarm last week at the results of a National Institute of Standards and Technology trial at Morgantown. Using a reader equipped with an antenna, NIST testers were able to lift 'an exact copy of digitally signed private data' from a contactless e−passport chip 30 feet away, said Neville

Pattinson, director of business development technology and government affairs for smart−card provider Axalto Americas.

The basic ICAO spec − the basis for the U.S.approach − does not require personal−data encryption. 'Unless the government reconsiders its current position and decides to add a security mechanism beyond the digital signature to its e−passport,' said Pattinson, the system will be insecure."

112. As world−renowned security technologist Bruce Schneier has said[65]:

"Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot of this is that travelers carrying around RFID passports are broadcasting their identity.

Think about what that means for a minute. It means that passport holders are continuously broadcasting their name, nationality, age, address and whatever else is on the RFID chip. It means that anyone with a reader can learn that information, without the passport holder's knowledge or consent. It means that pickpockets, kidnappers and terrorists can easily −− and surreptitiously −− pick Americans or nationals of other participating countries out of a crowd.

It is a clear threat to both privacy and personal safety, and quite simply, that is why it is bad idea. Proponents of the system claim that the chips can be read only from within a distance of a few centimeters, so there is no potential for abuse. This is a spectacularly naive claim. All wireless protocols can work at much longer ranges than specified. In tests, RFID chips have been read by receivers 20 meters away. Improvements in technology are inevitable.

Security is always a trade−off. If the benefits of RFID outweighed the risks, then maybe it would be worth it. Certainly, there isn't a significant benefit when people present their passport to a customs official. If that customs official is going to take the passport and bring it near a reader, why can't he go those extra few centimeters that a contact chip −− one the reader must actually touch −− would require?
...
Unfortunately, there is only one possible reason: The administration wants surreptitious access themselves. It wants to be able to identify people in crowds. It wants to surreptitiously pick out the Americans, and pick out the foreigners. It wants to do the very thing that it insists, despite demonstrations to the contrary, can't be done.

Normally I am very careful before I ascribe such sinister motives to a government agency. Incompetence is the norm, and malevolence is much rarer. But this seems like a clear case of the Bush administration putting its own interests above the security and privacy of its citizens, and then lying about it."

113. Obviously changes to the current privacy protection legislative regime would not make one scrap of difference to the situation that the legislature has allowed to occur with the *Australian Passports Act 2005*. Evidently, at present Australian citizens cannot trust even the legislature to protect them from arbitrary and unnecessary surveillance.

114. EFA is of the view that no legislation involving mandatory use or possession by citizens of technology with inherent privacy and security risks should be passed until the relevant government department has commissioned independent expert privacy and security impact assessments, published the resultant reports, obtained advice from the Federal Privacy Commissioner and undertaken wide public consultation. The public and the legislature would then be in a significantly better position to seek to ensure that only the least dangerous and invasive technology available to achieve the objective is used and that unnecessarily broad and vague powers are not granted to current and unknown future Ministers or other government personnel just in case they decide they want to use a different technology. EFA does not consider that disallowable legislative instruments are an adequate means of control in this regard.

115. Furthermore, while the Act and Explanatory Memorandum make references to the *Privacy Act 1988*, we consider any privacy protection that may be afforded by the *Privacy Act 1988* is likely to be weak at best. For example, it appears that any determinations made by the Minister permitting use and/or disclosure of personal information would be "authorised or required by law" and therefore permitted by the *Privacy Act 1988*. In our view, disallowable legislative instruments are not adequate in this regard either.

Go to Contents List

4.5 Online national ID 'Document Verification Service'

116. EFA notes with concern recent media reports regarding a proposed online national ID 'Document Verification Service' ("DVS"). For example, according to a report in The Australian IT[66]:

> *"...Federal cabinet will soon see a proposal for a national "document verification service" designed to combat identity−related crimes ranging from welfare fraud to terrorism.*
> *It would give federal and state government agencies and key businesses the right to verify the identity of clients by cross−checking birth certificates, drivers' licences and passports through a central data exchange hub.*
> *The Attorney−General's Department is finalising the proposal for the online system.*
> *The scheme has the same identification security goals as the Hawke government's politically unpalatable Australia Card proposal in 1987. ..."*

117. The government has apparently claimed that this scheme does not pose the same privacy risks as the failed Australia Card because it will not involve a unique identification number. However, that does not necessarily mean the risks are not the same. Data matching technology and systems have advanced markedly in the last twenty years. Furthermore, as discussed earlier herein, the Medicare smart card, with associated Medicare and HealthConnect numbers, has high potential to become a unique ID and commonly requested evidence of ID document, which would make data matching even easier. Further an "online" system poses additional privacy and security risks.

118. However, in the current total absence of publicly available information about how the DVS scheme would operate, it is impossible to determine the extent of privacy and/or security risks that it would pose, and whether the current privacy protection legislative regime is sufficient. However, it is most unlikely that the high level principles in the current legislation would be adequate. Most probably new, purpose−specific legislation would be necessary to strictly regulate access to and use of the system and information.

119. The total absence of public consultation and of publicly available information also makes it impossible to determine whether or not the DVS system should even be introduced. While improved methods of reducing identity theft and identity fraud are desirable, the secrecy with which the scheme has been developed to date gives rise to serious questions about whether it would in fact achieve the claimed objective and whether it is the least privacy invasive means available.

▲ Go to Contents List

---

5. Legislative changes to provide more comprehensive protection and improve the current regime

5.1 Requiring Technological Access Controls on Government Databases

120. EFA considers Principle 2 "Storage and security of personal information" of the PA, which applies to government departments/agencies, needs to be amended to require the implementation of technological access controls on government databases. Such controls are necessary to prevent access to personal information by public servants who do not need access to the particular records to undertake their duties.

121. In this regard, we note a recent disturbing decision by the NSW Administrative Decisions Tribunal concerning a parole officer who accessed personal information in the Department of Corrective Services database and disclosed it to other people. As reported in the Editorial of the Sydney Morning Herald (*'A question of privacy'*)[67] on 25 November 2004, the Tribunal:

> *"found that as a parole officer, Ms [M] was entitled to access the initial information about [the person], even though she was not [his] parole officer. However, it found that she was "acting in her private capacity" in giving that initial information to parents, and again in accessing the information about [the person's] visitors and contacting one. Strangely, it held that these "private" actions were not the responsibility of the department. The department's responsibilities were to put warnings on its computers about unauthorised access and this it had done."*

122. The Tribunal's decision[68] involved consideration of the "reasonable" security safeguards required by Principle 12(c) of the NSW *Privacy & Personal Information Protection Act 1998* ("PPIP Act")[69] which is effectively identical to Principle 4(a) of the Commonwealth *Privacy Act 1988*:

123. NSW Act:

> 12. Retention and security of personal information
> A public sector agency that holds personal information must ensure:
> ...
> c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse

124. Commonwealth Act:

> Principle 4 − Storage and security of personal information
> A record−keeper who has possession or control of a record that contains personal information shall ensure:
> (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse

125. The Tribunal found that merely the display of a "computer flag" informing public servants that information is confidential and must not be disclosed to unauthorized persons, nor accessed for personal reasons, is a sufficient security safeguard. Presumably a Federal Court would be likely to conclude the same in relation to the equivalent provision of the Commonwealth Act.

126. This situation is completely unsatisfactory in this day and age of ready availability of technological measures to prevent access. As the SMH Editorial concluded:

> *"... Putting aside questions about whether Ms [M] needed to access any files at all − could she not have taken her initial suspicions about [the person] to the police? − the wider issue raised by the case is why Corrective Services records are not restricted to those who need them. That would force others to make their ad hoc inquiries through proper channels. All government departments should encode data so it can be used only for its intended purpose. Anything less is an abject failure to protect privacy − and an invitation to blackmailers and vigilantes. Government departments might cast their minds back to 1995 when the Sydney detective Said Morgan retrieved from a police computer the address of a man who had molested his family, and shot him dead. A jury acquitted Mr Morgan of murder and manslaughter charges."*

127. It is also completely unsatisfactory that a government agency can escape responsibility for the actions of its staff by claiming they were acting in their personal capacity in accessing information on the department's database.

128. The Commonwealth Privacy Act needs to be amended as a matter of urgency to prevent a Federal Court from coming to the same conclusions as the NSW Tribunal.

129. We also note that in relation to specifically the Health Insurance Commission, it is required to establish detailed *technical* standards specifying access controls and limiting access to each database to those officers or contractors who have a reasonable need for access in order to ensure the effective administration of the particular program, etc.

130. HIC is also required to file a copy of the above Technical Standards Report with the Privacy Commissioner. However, the Auditor General's 2004−05 Report[70] states that:

> "5.45 ANAO requested HIC to provide a copy of the Technical Standards Report referred to in the Privacy Commissioner’s Guidelines. HIC was unable to locate a copy of the Technical Standards Report.
> 5.46 ANAO approached the OFPC seeking information on HIC’s lodgement, or otherwise, of the Technical Standards Report. The OFPC informed ANAO that it was unable to locate a copy of HIC’s Technical Standards Report ..."

131. Obviously when no−one can find a copy of the technical standards, neither HIC, the public, or anyone else can know whether or not HIC is complying with same.

132. Furthermore, the unknown technical standards were allegedly developed in February 1995. Amendments to the PA should also be made to require government agencies to review and update technological security measures more frequently than once every 10 years.

Go to Contents List

5.2 Requiring Security Safeguards on Government Issued Computer Chips

133. EFA considers there is also a need to amend IPP 4 to require government agencies to implement security safeguards protecting records on government issued computer chips, such as those to be on the Medicare smart card and in the new passports.

134. Currently IPP 4 requires a record−keeper "who has possession or control of a record that contains personal information" to implement security safeguards to protect that record against unauthorised access, use or disclosure, etc. However, when a record−keeper places a copy of such a record on a computer chip that is required to be held in the possession of members of the public, there is no requirement to implement security safeguards to protect that copy of the record against unauthorised access etc. IPP 4 should be amended to require security safeguards protecting records on government issued computer chips.

Go to Contents List

5.3 Improving the Definition of "Personal Information"

135. Currently the *Privacy Act 1988* ("PA") states:

> "*personal information* means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

136. A broader definition of "personal information" must be embraced in order to adequately protect individuals' privacy in the electronic information age. The current focus on identification as the basis for privacy protection is not adequate, nor was it adequate when the private sector provisions commenced in 2001.

137. The OFPC Issues Paper asks (p.21) "whether ability to contact or some additional approach should be taken to protect individual privacy". We consider that additional approach should be incorporated, however, that alone will not adequately protect individuals' privacy.

138. The definition must be extended to cover identifiers irrespective of whether it is obvious to the collector or discloser that an individual's identity can reasonably be ascertained from that identifier and whether or not an individual can be contacted by use of that identifier.

139. In the Internet environment there are a wider ranger of identifiers available than off−line, such as an Internet user's machine ID, IP address, user ID, email address, passwords, etc. Identifiers such

as these must be clearly incorporated within "personal information" protected by the Privacy Act and the Principles.

140. Aggregation of data can occur with minimal identifiers if one identifier is sufficiently unique to be cross−referenced with another.

141. Internet technologies enable the collection of information about individual Internet user's behaviour across thousands of web sites. Personal profiles about them, including their habits and interests, are being compiled surreptitiously and in many cases without users being aware that this is even possible, let alone their having provided their name to such web sites.

142. While many people appear to believe these profiles are only used for purpose such as targeting banner advertisements at particular Internet users and consider this to be of no concern, a far more disturbing aspect is that detailed profiles about consumers can make them more susceptible to discriminatory business practices such as redlining − the practice of placing particular customers at the end of a priority queue, or, of even greater concern, simply not dealing with them at all. As reported in "Weblining"[71] in BusinessWeek Online, 3 April 2000:

> *"Old−style redlining is unacceptable because it is based on geographic stereotypes, not concrete evidence that specific individuals are poor credit risks. Webliners may claim to have more evidence against the people they snub. But their classifications could also be based on irrelevant profiling data that marketing companies and others collect on the Web. How important to your mortgage status, say, is your taste in paperbacks, political discussion groups, or clothing? Yet all these far−flung threads are getting sewn into online profiles, where they are increasingly intertwined with data on your health, your education loans, and your credit history."*

143. On the Internet, it is not necessary for businesses or any other online service 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 be disclosed to other entities who are able to connect a "cyberspace" identifier with a name or other "real−world" identifier.

144. For further information on regarding online identifiers and associated privacy issues, see *Privacy Principles − irrelevant to cyberspace?*[72], Graham Greenleaf, Privacy Law & Policy Reporter (Prospect Publishing), 3 PLPR 114, September 1996.

145. EFA recommends that the definition of "personal information" in the PA be extended to include wording such as

> "any information which enables interactions with an individual on a personalised basis, or enables tracking or monitoring of an individual's activities and/or communication patterns, or enables an individual to be contacted"

146. In addition, the definition should be amended to include an explanatory note such as:

> "For the avoidance of doubt, in determining whether information is personal information, it is irrelevant that the identity of the individual may not be known or ascertainable by the collecting or disclosing organisation at the time of collection or disclosure."

5.4 Improving other provisions of the Privacy Act

147. In addition to the definition of "personal information", there are a considerable number of other aspects of the PA and the NPPs that require amendment to improve the operation of the regime. These are discussed in the section titled *Effectiveness of the Privacy Amendment (Private Sector) Act 2000*.

▲ Go to Contents List

5.5 Removing Inconsistencies between C'th Legislation

148. An additional means of improving the privacy protection provisions of the current regime would be to remove inconsistencies between Commonwealth legislation. For example, EFA is particularly concerned about the inconsistencies between the Part 13 privacy protections in the TA and the NPPs in the PA. A comparison and discussion of relevant provisions is provided in Appendix 1.

149. Also, the NPP 2.1(c)(i) direct marketing exemption is inconsistent with the Spam Act 2003 in relation to commercial electronic messages. This matter is discussed under the heading Direct Marketing Exemption later herein.

▲ Go to Contents List

---

6. Effectiveness of the Privacy Amendment (Private Sector) Act 2000

6.1 Exemptions

6.1.1 Small Business Exemption

150. EFA remains of the view, originally expressed in 2000, that the small business exemption should be deleted from the PA.

151. Small businesses comprise some 94% of Australian businesses, according to information provided by the Department of Employment, Workplace Relations and Small Business to the Standing Committee on Legal and Constitutional Affairs' inquiry into the provisions of the 2000 Bill.

152. Privacy rights do not disappear just because a consumer happens to be dealing with a small company. The responsibility upon commercial organisations to recognise the privacy rights of consumers does not magically become apparent when an organisation's revenue base exceeds some arbitrary figure. Individuals are rarely able to know whether or not an organisation is a small business for the purposes of the PA since annual turnover figures are rarely publicly disclosed.

153. We understand (from public comments made by the Federal Privacy Commissioner in late 2004) that there have been suggestions that the small business exemption be changed to apply to organisations with an arbitrary number of employees instead of an arbitrary annual turnover figure. We are opposed to an exemption based on number of employees because this would still result in exemption for organisations that collect and disclose substantial amounts and types of personal

information. Even a sole trader may collect, use and/or disclose large quantities of personal information, especially via, for example, an e−commerce web site.

154. At the very least, all small businesses involved in the telecommunications and Internet services sector must be required to comply with the NPPs. The limited privacy protection provisions of the *Telecommunications Act 1997* ("TA") do not cover *collection* of personal information at all. Further, as discussed in Section 4.1.1 in relation to the TA, individuals currently have less control and rights in relation to collection, use and disclosure of their personal information by small businesses in the telecommunications sector than they did before December 2001 when the ACIF industry code was de−registered by the ACA. That Code contained substantially the same provisions as the NPPs, together with related guidelines, and was enforceable by the ACA. It did not contain an exemption for small businesses.

155. Further, in conjunction with the *related body corporate/small business operator* provisions, this exemption could conceivably be used by large organisations with complex corporate structures to evade their responsibilities by transferring data collection activities to a smaller entity. (For further detail see the discussion about SBOs in section titled *Direct Marketing Exemption*).

156. EFA recommends that the exemptions for small businesses and small business operators be dropped.

▲ Go to Contents List

6.1.2 Related Bodies Corporate Exemption

157. EFA sees no justification for allowing organisations to escape compliance with some of the NPPs simply because they are part of a larger organisation. The exemption also enables large businesses to intentionally structure their affairs to enable avoidance of some of the NPPs.

158. Individuals often do not know that an organisation is related to another organisation and should not have to ask or attempt to investigate corporate structures in order to find out how far and wide their personal information could be spread.

159. The related bodies corporate exemption should be deleted. The same provisions should apply to related bodies corporate as to any other third party organisation.

▲ Go to Contents List

6.1.3 Political Parties Exemption

160. No justification has ever been provided for the exemption from the Act for political parties. Political parties should be treated no differently from any other organisation in respecting the privacy rights of Australian citizens. To do so is to send a message that the Privacy Act is only a token gesture, to be evaded when it happens to suit particular vested interests with the political clout to get their own way.

161. Among numerous other things the exemption allows political parties to collect information about citizens from third parties that could be completely wrong, and does not even grant citizens a right to know what that information is and have it corrected if it is not true.

162. The types and sources of information in political party databases has become increasingly known to the public (including very recently on *The National Interest* and in the *NT News*[73]), giving rise to even greater concern about this exception than five years ago.

163. EFA strongly objects to this exemption and considers it should be deleted.

▲ Go to Contents List

6.1.4 Direct Marketing Exemption

164. In relation to commercial electronic messages, the NPP 2.1(c)(i) direct marketing exemption is inconsistent with the *Spam Act 2003* in that it permits sending of such messages without consent, contrary to the *Spam Act*. At a minimum, NPP 2.1(c)(i) should be amended to be equivalent to the *Spam Act* in relation to consent.

165. In addition, the *Spam Act* is inconsistent with NPP 2.1(c) which appropriately requires all organisations sending direct marketing communications to inform the individual that they have the right to opt−out and provide details of how to do so. In contrast, the *Spam Act* inappropriately established a special class of senders who are authorised to send spam "relating to goods and services" and also a special class of exempt messages ("designated" commercial messages) and exempts those senders from the requirement to provide a means of opting out, i.e. functional unsubscribe facility. The *Spam Act* should be amended to require all senders to provide a functional unsubscribe facility and thereby remove the inconsistency with NPP 2.1(c)(iv) and (v).

166. We believe however that the direct marketing exception in the PA needs a complete overhaul as discussed below.

(a) Primary Purpose of Direct Marketing

167. As detailed later herein under *Primary and Secondary Purposes of Collection*, the NPPs do not regulate use and disclosure for the primary purpose of collection at all and organisations are free to collect personal information for any "primary purpose" they wish without consent.

168. Unless NPP 2 is amended to regulate use and disclosure for the primary purpose of collection (as recommended earlier herein), then the NPPs must be amended to prohibit collection without consent for the primary purpose of direct marketing.

(b) Secondary Purpose of Direct Marketing

169. The NPP 2.1(c) exception permitting secondary use of personal information for direct marketing without consent is totally unacceptable. It must be amended.

170. Personal information should only be used for marketing purposes with explicit consent, not by default with the blessing of the government. Unsolicited direct marketing, whether in the form of junk mail, telemarketing phone calls, junk fax, or by E−mail is notoriously unpopular with consumers.

171. The direct marketing exemption requires a consumer to be aware that they are permitting the use of their data (provided for the primary purpose of, e.g. purchasing a specific product) to also be

used for the secondary purpose of direct marketing unless they remember to specifically request not to receive direct marketing communications at the time of providing the information.

172. EFA considers this to be an unfair information practice which inadequately protects an individual's fundamental right to privacy. Remembering to opt out of direct marketing is unlikely to be foremost in a purchaser's mind when transacting a purchase and what is "impracticable" for an organisation in terms of seeking an individual's consent (NPP 2.1(c)(i)) is, to say the least, not clear and hence a matter of argument.

173. Furthermore, although the NPP permits the sending of direct marketing material once only (if the recipient then asks not to be contacted again), the NPPs only apply to "organisations" and the definition of an "organisation" excludes a "small business operator" (SBO), which is defined to be an entity that carries on one or more small businesses. Once one small business carried on by an SBO has collected an individual's address, each and every one of the other small business carried on by that SBO can send direct marketing material to the same individual who would, it appears, have to opt out each time (and the SBO businesses are not required to comply with the NPPs in any case). The SBO does not lose its exemption from the definition of "organisation" in the PA by disclosing the information to its small businesses nor by those businesses using the information for direct marketing. The exemption is only lost if the personal information is disclosed to "anyone else for a benefit, service or advantage". Disclosure to businesses within the SBO are not disclosures to "anyone else". Therefore, the collection of personal information by one small business can result in an individual receiving "once only" direct marketing material from numerous other businesses as a result of the collection of the information by one small business.

174. There appears to be no impediment to an SBO business disclosing personal information collected by them and contained in a direct marketing lists to unrelated third parties. While such a business would lose its exemption from "organisation" if it received a "benefit, service or advantage" in return, the damage would already have been done prior to the exemption being lost.

175. We recommend that the direct marketing exception be replaced with an "opt−in" provision that permits the use of personal information for direct marketing purposes only by specific prior consent. In addition, direct marketers should be required to provide "opt−out" instructions, each and every time they send direct marketing materials, not only the first time. Sanctions should be applied to breaches of these principles.

▲ Go to Contents List

6.2 Contractors

176. The section of the OFPC Issues Paper titled *Commonwealth Contractors* demonstrates the impracticability of having different sets of Privacy Principles applicable to government agencies and private sector organisations. Clearly the two different regimes need to be harmonised. We would support harmonisation provided that the outcome results in the highest level of privacy protection from each of the two existing regimes. We would not support an exemption for Commonwealth contractors who are small businesses or small business operators.

177. With regard to private sector contractors (as discussed in the OFPC Issues Paper under *Business efficiency and private sector contracting*), we consider this situation is another reason why the exemption for small businesses and small business operators should be deleted from the PA. In addition, we consider the PA should be amended to place obligations on organisations that engage

contractors to ensure the contractor only uses and/or discloses the personal information given to them for the purposes for which it is given and keep it secure, etc.

Go to Contents List

6.3 National Privacy Principles Generally

6.3.1 Primary and Secondary Purposes of Collection

178. As stated in the OFPC Issues Paper (p32) "[t]he NPPs do not specifically require organisations to get an individual's consent to collect personal information". In addition, the NPPs do not regulate the subsequent use or disclosure of information collected for the primary purpose of collection.

179. As a result, individuals have no choice or control whatsoever concerning collection, use and disclosure of their personal information for the primary purpose of collection. This situation is of greatest concern when organisations collect personal information from a third party, that is, without the knowledge, let alone consent, of the individual concerned.

180. EFA considers that NPP 2.1 should be amended to regulate use and disclosure of information collected for the primary purpose of collection. We see no legitimate reason for NPP 2 to apply only to use and disclosure for secondary purposes. Organisations should not be able to use personal information for either primary or secondary purposes unless the individual concerned would reasonably expect the organisation to use or disclose the information for the purpose or has consented to the use or disclosure for that purpose.

181. If NPP 2 is not amended as above, then at the least, it should be amended to prohibit use and disclosure for the primary purpose of collection in circumstances where the information was collected indirectly without consent, i.e. from a source other than the individual concerned without the consent of the individual, unless the use or disclosure is *essential* (requiring an objective test) for the provision of a service requested by the individual.

Go to Contents List

6.3.2 Bundled "Consent" and NPP 1.3 Notices

182. EFA considers the common organisational practices of requiring bundled "consent" and providing NPP 1.3 information in privacy policies that are changeable without any notice, let alone prior notice, are massively undermining the objectives of the PA.

183. Although the OFPC has widely promoted the PA with the slogan "My Privacy, My Choice", it has become apparent that a more truthful slogan may be "My Privacy, NO Choice".

184. In relation to the commentary concerning "bundled consent" in the OFPC Issues Paper (p32−33), we are of the view that such means of allegedly obtaining "consent" do not constitute consent to use and/or disclosure for secondary purposes. Individuals cannot give free and informed consent when they are presented only with broad and/or vague statements concerning possible uses and disclosures, and/or told that services will not be provided if they do not "consent" to the bundle. However, as we see no purpose in using bundles unless the organisation is assuming these result in valid consent, it would appear individuals' personal information is being used and disclosed for

purposes for which they did not consent and would not reasonably expect (i.e. in breach of NPP 2.1(a)).

185. Of additional concern is the common organisational practice of including NPP 1.3 information (about use and disclosure) in Privacy Policies that are changeable without any notice, let alone prior notice, to the individual. There appears to be no reason for this practice unless the organisation is mistakenly regarding same as sufficient for reliance on NPP 2.1(a)(ii), i.e. that "the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose". Moreover, as has been pointed out by the OFPC, expectation is more than awareness.

186. Until the above practices are stopped, individuals cannot have confidence that their privacy is respected, let alone protected.

187. **Examples of privacy policies changeable without notice:**

- Mobile Phone Service Provider, 14 Dec 2004:
  "[company] reserves the right to change this Privacy Policy at any time and notify you by posting an updated version of the Policy on its web site. The amended Privacy Policy will apply between us whether or not we have given you specific notice of any change. We encourage you to review this Privacy Policy periodically because it may change from time to time."[74]

  Note: The above policy was included in pre−paid mobile phone packs sold in shops in late 2004. Hence it appears that persons purchasing a mobile phone service need to have Internet access to find out whether the printed policy included with the product purchased has been changed.

- Telephone Service Provider, 14 Dec 2004
  "From time to time, it may be necessary for us to review our Privacy Awareness Policy. We reserve the right to amend our Privacy Awareness Policy at any time and to notify you by posting an updated version on the [company] website [company].com.au"[70]

- Marketer of leading brand name consumer products, 14 Dec 2004
  "...from time to time, our policies will be reviewed and may be revised. [company] reserves the right to change its Privacy Policy at any time and notify you by posting an updated version of the policy on its website.
  The amended Privacy Policy will apply between us whether or not we have given you specific notice of any change."[70]

- Australian Domestic Airline, 14 Dec 2004
  "We may amend this Privacy Statement as our business requirements or the law changes. Any changes to this Privacy Statement will be updated on [company].com and [company].com, so please visit [company].com or [company].com periodically to ensure that you have our most current privacy statement."[70]

- Bank, 14 Dec 2004
  "...In general, we will not use or disclose personal information collected about you **otherwise than for a purpose set out in this Privacy Policy**, for a purpose you would reasonably expect, a purpose required or permitted by law, or a purpose otherwise disclosed to, or authorised by, you. [emphasis added]

...
This statement sets out our current Privacy Policy. It replaces any of our other Privacy Policies or website Privacy Policy to date.
Please note that this Privacy Policy may change from time to time. ... We encourage you to periodically review our Privacy Policy for any changes."[70]

188. A further problem is that quite often policies of the above type have no date on them, nor do they highlight changes made since the previous version. Individuals who wish to know the details of the organisation's current policy therefore need to constantly re−read the entire policy.

189. In addition, there appear to be attempts to skate around the law (NPPs) via Privacy Policies. For example, a major telecommunications service provider's Privacy Policy[70] states:

> "[company] may Disclose Personal Information to unrelated third parties to enable outsourcing of functions (such as billing), where that is Disclosure or Use for a related Secondary Purpose and has been notified to individuals **or where such Disclosure is within the individual's Reasonable Expectations**...." [emphasis added]

and at the end of the above policy, in its glossary:

> "Reasonable Expectation means **a reasonable individual's expectation that their personal information might** be Used or Disclosed for the particular purpose."[70] [emphasis added]

190. However, NPP 2.1(a) does not refer to a phantom "reasonable individual's expectation", it refers to what the relevant individual would reasonably expect.

191. In our view, changes need to be made to the NPPs to ensure that:

- when information contained in NPP 1.3 and 1.5 notices concerning use and disclosure is insufficiently specific to enable the individual to give free and informed consent, or make an informed choice about whether to provide personal information, that the organisation cannot rely on NPP 2.1(a) to use or disclose the individual's personal information;

- privacy policies containing NPP 1.3 and 1.5 information must include the date of issue and changes made since the prior version must be highlighted or noted therein (e.g. a list of changed clause numbers and date of change at the end of the policy).

- any changes to NPP 1.3 and 1.5 information involving new uses or disclosure can not apply to previously collected personal information unless the organisation has directly notified the individual concerned of the changes and provided an easy to take up opportunity to opt−out of such new uses and disclosures or to terminate their relationship with the organisation without detriment.

Go to Contents List

6.3.3 Data Quality claimed as justification for Bundled "Consent"

192. NPP 3 − Data Quality − states:

> An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

193. We understand that the accuracy requirement of NPP 3 is being used by some organisations as an alleged justification for their use of bundled "consents". For example, during a meeting convened by the OFPC in November 2004, a representative of a mobile telephone call service provider said the organisation used bundled consents to minimise the amount of data needing to be entered into its information systems and had recently re−designed those systems to reduce the amount of data entry required. This was said to be necessary to increase the probability of accuracy of data, that is, to reduce opportunity for inadvertent errors during data entry.

194. Such an interpretation of the NPP 3 accuracy requirement is plainly contrary to the intent and objectives of the PA.

195. NPP 3 must be amended to make clear that it cannot be used as an excuse for giving individuals less choice in relation to the use and disclosure of their personal information.

▲ Go to Contents List

6.3.4 Use & Disclosure by Secondary Collectors

196. NPP 2 should be amended to explicitly place restrictions on use and disclosure by secondary collectors, that is, organisations that have collected personal information from another organisation. Secondary collectors should be prohibited from using or disclosing information for purposes other than those for which the disclosing organisation is permitted to use or disclose the information.

▲ Go to Contents List

6.3.5 Collection of Unlawfully Disclosed Personal Information

197. We understand the OFPC has said (during investigation of a currently unresolved complaint[75]) that collection of personal information that has been unlawfully disclosed by another party might not constitute a collection by unfair or unlawful means under NPP 1.2 and that subsequent use, and disclosure to one or more other organisations, might not constitute breach of NPP 2.

198. Such an interpretation of NPP 1.2 and NPP 2 undermines the objectives of the PA to the extent that individuals are afforded no control whatsoever in relation to collection, use and disclosure of their personal information where that information was unlawfully disclosed in the first place.

199. The unsatisfactory implications of such an interpretation are especially apparent when considering a case where the primary purpose of the secondary collection is direct marketing. For instance, Organisation A unlawfully discloses personal information to Organisation B, and Organisation B's primary purpose of collecting that unlawfully disclosed information is direct marketing. Organisation B would then free to disclose the information to one or more further organisations for direct marketing purposes, so a third organisation would be free to disclose it to a

fourth and so on, notwithstanding that the information was only able to be collected, used and disclosed by the second and subsequent organisations as a result of the breach of NPP 2 by the initial collector.

200. If, as has been suggested, NPP 1.2 and NPP 2 can be interpreted as permitting the above scenario, it demonstrates such a massive "hole" in the protection offered by the PA that it cannot have been intended.

201. It is not as if there is some sort of property "title" in individuals' personal information that can be restored to them after discovery (if ever) of the initial unlawful disclosure. That is, personal information cannot be restored to the "owner" in a similar way to stolen goods. Once information about them has escaped "into the wild", an individual has no control whatsoever.

202. The privacy interest supported by the Act is that of the subject person concerned who should have some assurance that the limited promise of protection under that law is actually applied, not avoided by sleight of hand or regulatory acceptance of routine "laundering" of unfairly or improperly collected data through intermediaries or "outsourcing".

203. Furthermore, if it is *necessary* (NPP 1) for an organisation to collect unlawfully disclosed personal information, then as a matter of general principle such organisations should not be in business or should be required to find a new business model. NPP 1.1 and 1.2 should be interpreted in a manner that discourages such privacy invasive business models. It is not an undue burden on legitimate businesses to require them to only collect and use lawfully disclosed personal information.

204. The NPPs must be amended to eliminate any potential for an interpretation that means, in effect, "an unlawful step in the initial collection process does not mean it was collected unlawfully by the subsequent collector/s, nor that it was used or disclosed unlawfully by those collector/s". In particular, the NPPs must be amended to:

- prohibit knowing collection of unlawfully disclosed information; and
- make awareness by the collecting organisation that the personal information may have been unlawfully disclosed a relevant consideration in deciding whether collection has been by fair means; and
- require organisations to destroy information that has been unlawfully disclosed to them once that organisation becomes aware of the unlawful disclosure.

205. In addition, NPP 1 should be amended to specifically require that collection be for a lawful purpose. Presently NPP 1.2 only requires that the means of collection be lawful.

▲ Go to Contents List

6.3.6 Definition of Direct / Indirect Collection

206. NPP 1.4 states:

> If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

207. We understand that during investigation of a currently unresolved complaint[76] by the OFPC it has been suggested that NPP 1.4 refers to collection of personal information **directly** from the individual and that an individual's consent or express denial of consent to collection is irrelevant to the question of whether NPP 1.4 has been breached in collecting information from a third party.

208. Such an interpretation has been used in an attempt to show no breach of NPP 1.4 when an individual's personal information has been collected from a third party, despite the individual concerned having previously expressly denied consent to the third party to disclose the information and the collecting organisation having the contact details of the individual (their customer) enabling them to seek the individual's consent to receive the information from the third party.

209. As NPP 1.4 does not include the word "directly" and the above interpretation is so contrary to the overall intent of the PA, in our view, the interpretation cannot be correct. Nevertheless, it is apparent that NPP 1.4 needs to be amended to prevent such an interpretation.

210. In addition, an interpretation implying "directly" has undesirable consequences that make it unnecessarily difficult for individuals to provide, and organisations to legitimately collect, personal information without breaching NPP 1.4. In this regard, we consider it is necessary in interpreting NPP 1.4 to distinguish the means of collection (the communications chain, which may involve one or more third parties) from the relationship. The wording "only from that individual" must refer to the relationship and not the communications chain − otherwise all sorts of contemporary transactions would be prohibited. For example:

- If consent is regarded as totally irrelevant to NPP 1.4, then even where an individual wishes to voluntarily give consent to Organisation A to disclose their personal information to Organisation B, Organisation B must not collect that information if it is reasonable and practicable to collect the information from the individual. We consider it highly unlikely that is the intent of NPP 1.4.

- An interpretation implying "directly", as in the instance referred to above (which concerns telecommunications businesses), would equally apply to collection of personal information from, for example, an email message. That is, that the recipient of the email message is not collecting the information **directly** from the individual, but from the third party carriage service provider (carrier/ISP) who provides the recipient's incoming mail box from which the recipient retrieves the information. In other words, the above interpretation of NPP 1.4 appears to result in the situation that where it is reasonable and practicable to collect the information **directly** from the individual, e.g. in person or by a real−time voice call, then email must not be used. We consider it highly unlikely that is the intent of NPP 1.4.

▲ Go to Contents List

6.3.7 Anonymity

211. NPP 8 − Anonymity − states:

> Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

212. We understand, in relation to a currently unresolved complaint[77], that it has been argued that a disclosing organisation has no responsibility to facilitate anonymous transactions, that is, that the entire responsibility lies with the collecting organisation.

213. We submit that such an interpretation of NPP 8 is incorrect and that NPP 8 needs to be amended to clarify that the obligation is to wherever possible (lawful and practicable) facilitate anonymous transactions, including with other organisations.

214. We note the advice in the OFPC Consultation Paper on the draft NPP Guidelines[78] that:

> "NPP 8 along with NPP 1.1 seeks to reverse through law the trend in new and existing information systems to collect more personal information than is necessary for a transaction" and in relation to what is impracticable that "additional cost, inconvenience ... will not be sufficient grounds".

215. With the increasing use of technology and automated information systems, in the absence of a shared responsibility by the disclosing organisation, there is a high risk that NPP 8 will be totally ineffective. Collectors are likely to claim that because the discloser sends them information and the technology in use by the recipient/collector automatically collects the information, it would be "impracticable" for the collector to comply with NPP 8.

216. An interpretation of NPP 8 that places no responsibility on the discloser, and also enables the collector to claim "impracticability" where the disclosure and subsequent collection is carried out by automated technological methods, would have widespread ramifications for the protection of individuals' privacy in the many circumstances where electronic information systems and communications systems are used. Not only would non−compliance with NPP 8 become more widespread, but information and communications systems will continue to be intentionally designed, and/or intentionally configured, to prevent individuals from being able to choose to be anonymous, contrary to one of the objectives of NPP 8 stated in the OFPC Consultation Paper.

217. Further, whether or not it is "impracticable" for the collector to comply in any particular instance, it is certainly impractical, and quite often impossible, for the individual concerned to have sufficient knowledge about a particular technology or information system to support a complaint concerning breach of NPP 8 on the grounds that it is practicable for the organisation to comply.

218. We submit that NPP 8 needs amendment to clarify that the responsibility to facilitate anonymous transactions is shared by the disclosing and collecting organisations. In addition, NPP 8 should be amended to place a specific obligation on organisations to design and build their information and communication systems to facilitate anonymous transactions.

▲ Go to Contents List

6.3.8 Transborder Data Flows

219. EFA is concerned that NPP 9 may not effectively protect individuals' personal information. Further, even if it does, individuals rarely have any way of knowing in advance whether their information will be disclosed to overseas organisations (so they have no choice), nor whether appropriate protections exist in the foreign country's law or have been put in place by the Australian organisation.

220. The increasing use of overseas call centres, for example by Australian credit card providers, is of significant concern. Staff in such call centres obviously have access to credit card details and transaction histories, etc.

221. In our view, the NPPs should be amended to require organisations to:

- provide prior notice (i.e. before collection) to individuals that their information will be sent to a foreign country, and/or that the individual will be required to deal with customer enquiry/support centres located in a foreign country; and
- provide notification of the means by which the Australian organisation has ensured their personal information will be effectively and adequately protected;
- unless:
    - ♦ the overseas organisation is subject to a law which is substantially similar to the private sector provisions of the PA; or
    - ♦ the individual concerned has consented to the transfer.

▲ Go to Contents List

---

7. Powers & Resourcing of the Office of the Federal Privacy Commissioner

222. We remain of the view expressed in 2000 that a major weakness in legislation is the lack of adequate enforcement provisions. We consider the PA should contain enforcement mechanisms that persuade compliance from both big business and small business.

223. We note the discussion concerning enforcement mechanisms in the OFPC Issues Paper (p47) and advise that in our view:

- the Commissioner should be given additional powers, for example, to ask organisations to commit to an undertaking that would be enforceable in the courts, or to issue a standard or binding code;

- the Commissioner should be given powers to enforce compliance with the PA where a breach has been found as a result of his or her 'own motion' investigation into the practices of private sector organisations;

- the Commissioner should be given power to proactively audit private sector organisations' compliance with the NPPs;

- the Commissioner's office should be provided with adequate funding to exercise the above additional powers.

224. With regard to the Commissioner's 'own motion' investigations, the need for enforcement powers is particularly evident in cases where it is known that a privacy breach has occurred but the subject individuals do not know whether personal information about them was involved, therefore they cannot make a formal complaint that their privacy has been unlawfully breached. For example, according to a recent report in The Australian[79], personal information about Acer's customers was exposed on Acer's online shopping web site, however the OFPC said its powers to take action against Acer were limited in the absence of a formal complaint about the incident.

225. It has also long been of major concern to EFA that:

> "[T]here is no right of review of the substance of a Commissioner's determination ... Respondents have the possibility of having a case hear [sic] afresh by refusing to comply with a determination and waiting for the Commissioner to seek to have the case enforced in court. However, this strategy is not available to an aggrieved complainant." (OFPC Issues Paper p30)

226. This unsatisfactory situation should be removed by amendments giving both complainants and organisations the right to appeal to the Administrative Appeals Tribunal and have the matter heard afresh.

227. In relation to the complaints process, we note the following remarks in the OFPC Issues Paper (p30):

> "There may be concerns that the complaints process lacks transparency because the confidential nature of conciliation settlements means that the nature of breaches, and the Office's view about the application of the NPPs, is hidden from public scrutiny.
>
> It may be argued that individuals' ability to exercise their rights is impeded by the Office's focus on conciliation in handling complaints. Individuals may not be in a position to negotiate their interests effectively in this process. In the absence of understanding the basis on which cases have been decided or resolved in the past, they may be negotiating in a vacuum."

228. We have the above concerns arising from the situation in relation to complaints known to us. We consider the complaints process needs greater transparency and considerably more information about the OFPC's views about application of the NPPs needs to be made publicly available.

229. We are also concerned by the delays in dealing with complaints apparently due to inadequate funding of the OFPC. We consider the OFPC should be sufficiently well−funded to deal with complaints promptly, and without needing to remove staff from other important areas such as policy and auditing of government agencies as has reportedly occurred.

230. Without adequate complaints handling procedures, backed up ultimately by strong legal sanctions, the PA will continue to be a generally ineffective and token piece of legislation.

▲ Go to Contents List

8. Conclusion

231. The operation of the private sector provisions over the past three years has predictably shown that the limited privacy protections allegedly offered are a totally inadequate response to consumer privacy needs in the 21st century.

232. The definition of "personal information" in the PA is inadequate in context of the electronic environment.

233. The legislation contains too many exemptions and exceptions. In addition, numerous

provisions of the PA and the NPPs are lacking in clarity and ambiguities are being exploited in ways contrary to the stated intent of the legislation. There is increasing evidence that even the regulator is interpreting the NPPs in the least privacy protective manner possible. Furthermore, enforcement provisions in the legislation are inadequate.

234. Instead of empowering individuals to exercise their right to privacy of personal data, and choice about how that data may be collected, used and disclosed, the legislation confers on certain business interests the right to invade individual privacy.

235. Finally, we consider the OFPC's use and promotion of the slogan "My Privacy, My Choice" to be highly misleading at best. In our view, use of the slogan should cease until such time as a major overhaul of the legislation has been undertaken and implemented that results in the slogan expressing fact instead of wishful thinking.

▲ Go to Contents List

Appendix 1

Comparison of *Telecommunications Act 1997* (Part 13) and *Privacy Act 1988* (NPPs)

1. As mentioned in Section 4.1.1, the *Telecommunications Act 1997*[1] ("TA") contains a number of exceptions to the Part 13 privacy protections that are inconsistent with the *Privacy Act 1988*[2] ("PA") without justifiable reason.

2. We discuss below provisions of the TA that now in effect authorise breach of the NPPs, although prior to the 2001 Privacy Act amendments the breadth of these exceptions in the TA were limited by a registered and enforceable industry code which was substantially the same as the NPPs.

Contents:

Consent, knowledge, awareness, reasonable expectations

3. This section discusses the following provisions of the TA and PA:

TA: 289 Knowledge or consent of person concerned
Division 2 does not prohibit a disclosure or use by a person of information or a document if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the other person:

(i) is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned; or

(ii) has consented to the disclosure, or use, as the case requires, in the circumstances concerned.

PA NPP: 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

4. During a November 2004 meeting convened by the OFPC at the Melbourne office of the Australian Communications Authority ("ACA"), a representative of a large telecommunications service provider expressed the view that there is little difference between s289 of the TA and NPP 2.1 of the PA, that is, that they are not inconsistent. We disagree with that view as discussed below.

5. In the case of use or disclosure for the **primary purpose** of collection, the TA (s289) is more protective than the PA (NPP 2). The TA restricts use or disclosure for the primary purpose to circumstances of which the individual is "reasonably likely to have been aware" or has consented. In contrast, NPP 2 does not restrict use or disclosure for the primary purpose at all.

6. However, in the case of use or disclosure for a **secondary purpose** of collection, the TA is significantly less protective than the PA.

7. NPP 2.1 prohibits use or disclosure 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" (or has consented).

8. In contrast the TA (s289) authorises use and disclosure when the individual is merely "reasonably likely to have been aware" that the information is usually disclosed or used for the secondary purpose/s (or has consented). Hence, it appears that businesses in the telecommunications sector can merely notify individuals they use and disclose personal information (including sensitive information) for numerous stated secondary purposes (including purposes unrelated to the primary purpose and that the individual would not reasonably expect), thereby making it "reasonably likely" that the individual has been "made aware". Further there is no requirement that the individual actually be "made aware", nor that they were "reasonably likely to have been aware" ***before*** their personal information was collected.

9. As has previously been pointed out by the OFPC:

> "Expectation is more than awareness. Telling an individual in NPP 1.3 information or by some other method about the proposed secondary use or disclosure is not necessarily enough to create a reasonable expectation although it may help."
> and
> "In applying NPP 2.1(a) the Commissioner suggests that it may help an organisation if it considers whether a reasonable individual in the circumstances, if asked, would have agreed to the proposed use or disclosure." (OFPC Consultation Paper on the draft National Privacy Principle Guidelines, 7 May 2001[78])

10. Moreover, that NPP 2.1(a) requires more than an individual being "reasonably likely to have been aware" (s289 of TA) is made plain in the PA Explanatory Memorandum (2000) which states:

> "The 'reasonable expectations' test would be applied from the point of view of the person in the street, that is, an organisation should be able to use or disclose personal information in ways in which a person with no special knowledge of the industry or activity involved, would expect. For example, if a person has several different types of contact with one bank, he or she could expect the information about themselves to be shared within that bank. If the banking group also ran a health insurance business, the individual would not expect their health claims record to be matched with banking information."

11. EFA submits that either the PA or TA must be amended to require businesses in the telecommunications sector to comply with NPP 2.1(a) in relation to use and disclosure for **secondary** purposes, that is, so that TA s289 ceases to authorise breach of NPP 2.1(a). In so doing, the long existing protection of the TA in relation to use and disclosure for the **primary** purpose must not be removed or made any weaker.

Unnecessary collection, use and/or disclosure without consent

12. This section discusses the following provisions of the TA:

> **TA:** 291 Business needs of other carriers or service providers
> (1) Section 276 does not prohibit a disclosure or use by a person of information or a document if:
> (a) the disclosure or use is made by or on behalf of:
> (i) a carrier (the first carrier); or
> (ii) a carriage service provider (the first provider); and
> (b) the disclosure or use is made for a purpose of, or is connected with, any other carrier or service provider carrying on its business as such a carrier or provider; and
> (c) the information or document relates to a person (the third person) who is a customer or former customer of:
> (i) the first carrier or the first provider; or
> (ii) the other carrier or the other provider; and
> (d) the disclosure or use is made for a purpose of, or is connected with:
> (i) the supply, or proposed supply, by the other carrier or other provider to the third person of a carriage service or a content service; or
> (ii) the supply, or proposed supply, by the other carrier or other provider to the third person of goods or services for use in connection with the supply of a carriage service or a content service; or
> (iii) the installation, maintenance, operation or provision of access to a telecommunications network or a facility, where the network or facility is used, or for use, by the other carrier or the other provider to supply a carriage service or a content service to the third person.
>
> 291(2) and (3) [contain similar exceptions to 291(1) above concerning intermediaries, resellers, contractors etc]

13. The s291 exemption in the TA is vastly less privacy protective than the PA, if the interpretation of the law being used by some telecommunications service providers and the Australian Communications Authority ("ACA") is correct. Whether or not their interpretation is correct (and we believe it is not), the law should be clarified to provide at least equivalent protection to that of NPP 2.

14. According to the opinion of the ACA included in a complaint decision issued in August 2004, s291 authorises businesses in the telecommunications sector to:

- use and disclose personal information without the subject individual even being "made aware" including:
  - ♦ use and disclose personal information about individuals who are **former** customers of the disclosing business, including when that business has collected the personal

information from a third party many years **after** the individual ceased to be a customer of that business

- ♦ disclose personal information about individuals who are not customers of the business to which it is disclosed and who have no wish to become a customer of that business (e.g. disclosure to another business for the recipient business's direct marketing purposes)
- ♦ disclose personal information that is **not** necessary for one of the recipient business's, functions or activities. According to the ACA's decision, the s291 exception does not involve a needs test notwithstanding that the intent of the exception is plain in the section title *Business needs of other carriers or service providers*.

15. We believe the ACA's opinion is wrong because among other things their analysis failed to take into account the fourth element (clause (1)(d)) of s291 which must be satisfied for the s291 exemption to apply. More detailed information on this matter has been provided to the OFPC in a representative complaint[17] (OFPC Reference C6951).

16. Irrespective of the correct interpretation, it is fact that some telecommunications service providers are relying on s291 to use and disclose personal information in circumstances that would otherwise be in breach of NPP 2 and that are very unlikely to have been intended by the Parliament in enacting s291 of the TA. Such use and disclosure is also contrary to previous interpretations of s291 made publicly available by the ACA and TIO, for example:

- Previously ACA registered ACIF Industry Code−*Protection of Personal Information of Customers of Telecommunications Providers*[4] (p18)
  "...section 291 of the Act...allows uses for the business needs of other carriers or service providers (which would generally be accompanied by a disclosure...) that are associated with providing a service **to the person who is the subject of the information or document**. This provision is designed to allow uses/disclosures which are 'triggered' by some action or request by a customer such as dialling an access Code to make use of another carrier." (emphasis added)

  (Notably, in relation to the complaint referred to earlier herein, Telstra commenced disclosing personal information in circumstances other than the above three months after the Code was de−registered. The relevant Telstra service had operated without such disclosures since November 2000, at which time the Code was registered.)

- ACA Telecommunications and Law Enforcement Manual[20]
  "to permit a carriage service intermediary to pass on the details of a customer to a network operator so as to permit connection. Disclosures would also be permitted where a customer changes his or her CSP."

- TIO Position Statement, 2003[21]
  to allow a "provider who has the customer's details to disclose the customer's information to another provider [e.g. a 190 calls provider] so that it can bill for the calls made"

17. In our view, either the PA or TA must be amended so that *all* businesses in the telecommunications services industry are required to comply with NPP 1 in relation to *necessary* collection and NPP 2 in relation to use and disclosure, so that TA s291 (and the related s302 secondary use/disclosure exceptions) cannot be interpreted or applied in a way that authorises breach of NPP 2 of the PA.

Personal Information about third parties in communications

18. This section discusses the following provisions of the TA:

> **TA:** 290 Implicit consent of sender and recipient of communication
> Section 276 does not prohibit a disclosure or use by a person if:
>
> (a) the information or document relates to the contents or substance of a communication made by another person; and
>
> (b) having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use.

19. This exception, on its face, appears to result in inadequate protection for personal information about third parties referred to in a communication. The exception should be amended to ensure that telecommunications businesses cannot disclose personal information about third parties based on an assumption that other persons (the sender and recipient) would have consented.

20. We note that the de−registered ACIF Code states that s290 "is intended to allow disclosure of public communications, for example, where a carrier discusses the content of an on−line bulletin board, or the content of a pay−television program carried on a cable network". However, that interpretation is not obvious from s290 itself. In the absence of a registered industry Code, and with increasing numbers of new entrants including small businesses in the telecommunications industry, it is doubtful that s290 would always be interpreted as said to have been intended in a de−registered code.

Authorisation by or under law

21. This section discusses the following provisions of the TA and PA:

> **TA:** 280 Authorisation by or under law
> (1) Division 2 does not prohibit a disclosure or use of information or a document if:
>
> (a) in a case where the disclosure or use is in connection with the operation of an enforcement agency−the disclosure or use is required or authorised under a warrant; or
>
> (b) in any other case−the disclosure or use is required or authorised by or under law.
>
> (2) In this section:
> enforcement agency has the same meaning as in section 282.
>
> **PA:** NPP 2.1
> (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
> (g) the use or disclosure is required or authorised by or under law; or
> (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
>
> (i) the prevention, detection, investigation, prosecution or punishment of

criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
(iii) the protection of the public revenue;
(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

...
Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

22. The private sector amendments to the PA inserted then new s303B into the TA which states that exceptions to the Part 13 privacy protections of the TA are taken to be "authorised by law" for the purposes of the PA (NPP 2.1(g) contains an exception for use or disclosure that "is required or authorised by or under law"). It is thus clear that the specific exceptions in Part 13 of the TA over−ride the privacy protections of the PA.

23. However, Part 13 of the TA also contains an exception for "disclosure or use [that] is required or authorised by or under law" and in our opinion it is not sufficiently clear that the list of exceptions in NPP 2 of the PA do not over−ride the specific privacy protections of Part 13 of the TA.

24. We believe the PA needs to be amended to make clear that NPP 2.1 does not authorise use or disclosure that would otherwise be in breach of the TA. Alternatively, s280 of the TA needs to be amended to state that s280(1)(b) does not authorise uses or disclosures that are authorised by NPP 2.1 of the PA.

Recommended Solution to Part 13 Inadequacies

25. While EFA considers that the TA requires amendments to address the above mentioned inadequacies, we would not support removal of Part 13 of the TA (for example, to replace it with reference to the NPPs and PA).

26. The telecommunications industry, and especially carriage service providers, of necessity have access to vastly more information about individuals than do most private sector organisations. The information held by them, and accessible to them as it passes through their networks, includes information about not only their own customers but also about members of the public in general, including the content of their communications. As such, the telecommunications industry is a special type of industry that the Parliament has long recognised should be subject to special obligations to protect privacy and that recognition resulted in the enactment of the Part 13 obligations and responsibilities many years ago.

27. Further, Part 13 deals with many aspects of the telecommunications industry that are specific to that industry and that are not addressed at all, let alone adequately, by the high level NPPs. These include not only obligations to protect privacy but also detailed rules concerning use and disclosure

of information for specifically authorised purposes such as to law enforcement agencies and emergency services, etc. In our view, it would not be practical or desirable to replace or substantially change Part 13.

28. In summary, we are of the view that the telecommunications industry must remain subject to Part 13 of the TA which contains significantly more specific and detailed obligations and responsibilities in relation to use and disclosure of information than is provided by the high level NPPs. However, Part 13 should be amended to address the inadequacies in privacy protection discussed above.

Go to Contents List

References

1. *Privacy Act 1988*
<http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm>

2. *Telecommunications Act 1997*
<http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm>

3. Australian Communications Authority: Replaced and removed industry codes
<http://internet.aca.gov.au/ACAINTER.2293792:STANDARD:1686360264:pp=DIR3_14,pc=PC_2132>

4. ACIF *Industry Code − Protection of Personal Information of Customers of Telecommunications Providers*, Australian Communications Industry Forum (ACIF)
<http://internet.aca.gov.au/acainterwr/telcomm/industry_codes/codes/c523b.pdf>

5. *Issues Paper: Review of the Private Sector Provisions of the C'th Privacy Act 1988*, Office of the Federal Privacy Commissioner (OFPC), October 2004.
<http://www.privacy.gov.au/act/review/index.html>

6. *OzEmail − an ISP's approach to privacy*, Justin Milne−OzEmail, Privacy Law and Policy Reporter 26, 2000.
<http://www.austlii.edu.au/au/journals/PLPR/2000/26.html>

7. *Online research a wise hit*, Louise Hattam, Herald Sun Melbourne (Business, p25), 19 July 2004

8. *Bright future for online banking*, Adrian Giles [founder and director of Hitwise], WebHead Magazine, ZDNet Australia, 26 September 2001.
<http://www.zdnet.com.au/news/business/0,39023166,20260621,00.htm>

9. *Heavyweights back Sinewave*, by Jane Schulze, The Age (Business, p5), 13 July 2000.

10. "About Hitwise Australia" page, as at 16 Dec 2004
<http://www.hitwise.com.au/about/>

11. Hitwise Methodology FAQ, as at 2 Dec 2004
<http://www.hitwise.com.au/faq/?currentfaq=Methodology>
(Note: The content of the above page no longer refers to IP addresses. The page has been changed since 2 Dec 2004, perhaps not coincidentally shortly after some members of the public and journalists started asking questions about Hitwise's collection and use of information from ISPs).

12. Hitwise Privacy Statement, as at 16 Dec 2004
<http://www.hitwise.com.au/info/privacy.html>

13. See note 7.

14. *Telecommunications (Interception) Act 1979*
<http://www.austlii.edu.au/au/legis/cth/consol_act/ta1979350/>

15. *Web stats firm in flap over 'packet sniffing'*, Sam Varghese, Sydney Morning Herald, 10

December 2004.
<http://smh.com.au/news/Breaking/ Web−stats−firm−in−flap−over−packet−sniffing/ 2004/12/10/1102625508288.html>

16. Hitwise Pty Ltd Patent Application: *Method and System for Characterization of Online Behaviour*
<http://v3.espacenet.com/textdes?DB=EPODOC0;

17. Representative complaint to ACA concerning disclosure of silent and other blocked calling number information to ISPs, and copy of ACA decision, July 2003 − August 2004.
<http://www.efa.org.au/Issues/Privacy/cni−complaints/index.html>

18. *ACA issues warning on silent and blocked numbers*, Australian Communications Authority, Media Release, 26 August 2004.
<http://internet.aca.gov.au/ ACAINTER.3997752:STANDARD:616463804:pp=DIR1_128,pc=PC_1086>

19. See note 4.

20. Australian Communications Authority, *Telecommunications and Law Enforcement Manual* (875 Kb)
<https://www.aca.gov.au/aca_home/licensing/radcomm/about_radcomms_licensing/leac.pdf>

21. TIO Position Statement: Customer's personal information passed to another provider, 2003.
<http://www.tio.com.au/POLICIES/Privacy/Customer's%20personal%20information%20passed %20to%20another%20provider.htm>

22. EFA submission to Australian Communications Authority re *Who's Got Your Number?: Regulating the Use of Telecommunications Customer Information*, 14 May 2004.
<http://www.efa.org.au/Publish/efasubm−aca−ipnd.html>

23. Australian Communications Authority, *Who's Got Your Number?: Regulating the Use of Telecommunications Customer Information*, 18 March 2004.
<http://internet.aca.gov.au/acainterwr/telcomm/industry_standards/ customer_info_disc_paper.pdf>

24. EFA submission to the Inquiry into the Provisions of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* conducted by the Senate Legal & Constitutional Legislation Committee, 28 June 2004.
<http://www.efa.org.au/Publish/efasubm−slclc−tiabill2004−sc.html>

25. Senate Privileges Committee, *Execution of Search Warrants in Senators' Offices − Senator Harris − 114th Report*, tabled 20 August 2003.
<http://www.aph.gov.au/senate/committee/priv_ctte/report_114/report.pdf>
Clerk of the Senate, Submission to Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation, 2004.
<http://www.aph.gov.au/senate/committee/scrutiny/inquiries/submissions/ entry_search/sub02.pdf>

26. Australian Law Reform Commission 1995, Report No. 74: Designs, Chapter 14
<http://www.austlii.edu.au/au/other/alrc/publications/reports/74/ ALRC74Ch14.html#ALRC74Ch14AntonPillerorde>

27. *Anton Piller Orders: From T−Shirts to MP3s*, Seet, S and Kennedy, F (Gilbert and Tobin Lawyers), 6 November 2003.
<http://www.gtlaw.com.au/t/publications/default.jsp?pubid=498>

28. EFA submission to the Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation conducted by the Senate Standing Committee for the Scrutiny of Bills, 26 July 2004.
<http://www.efa.org.au/Publish/efasubm−ssbc−search2004.html>

29. *Sony v University of Tasmania* [2003] FCA 532
<http://www.austlii.edu.au/au/cases/cth/federal_ct/2003/532.html>

30. *Privacy v Intellectual Property litigation: preliminary third party discovery on the Internet*, Nic Suzor, Australian Bar Review, Vol. 25, p. 228, 2004

31. See note 30.

32. See note 29.

33. See note 30.

34. Federal Court of Australia, Practice Note No. 10 − Anton Piller orders, issued by the Chief Justice, 8 April 1994.
<http://www.fedcourt.gov.au/how/practice_notes_cj10.htm>

35. See note 28.

36. See note 28.

37. EFA submission to the Inquiry into the *Spam Bill 2003* and *Spam (Consequential Amendments) Bill 2003* conducted by the Senate Environment, Communications, Information Technology and the Arts Legislation Committee, 20 October 2003.
<http://www.efa.org.au/Publish/efasubm−ecitaspam.html>

38. *Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme*, Roger Clark, 1987
<http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html>

39. Senate Hansard, Answer to (previous) *Question without Notice: National Health Communications Network*, 17 September 1992
<http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=317498t;

40. *Proof of ID required? Getting Identity Management Right*, Malcolm Crompton, former Federal Privacy Commissioner, speech delivered to the Australian IT Security Forum, Sydney, 30 March 2004.
<http://www.privacy.gov.au/news/speeches/sp1_04p.html>

41. SchlumbergerSema (now Atos Origin) Response to the UK Government's consultation paper 'Entitlement Cards and Identity Fraud', January 2003
<http://web.archive.org/web/20030727131743/http://www.schlumbergersema.com/ukn/publicsector/entitlement
<http://www.atosorigin.co.uk/industries/publicsector/idcards/docs/AtosOrigin_Identity_Card_Identity_Fraud−1.

42. VicRoads: Introducing New Driver Licence Technologies − A Smarter Licence for Victorians, March Consulting Pty Ltd, June 2002
<http://www.egov.vic.gov.au/pdfs/final200102%20report.pdf>

43. The Auditor−General, Audit Report No.24 2004–05, *Integrity of Medicare Enrolment Data, Health Insurance Commission*
<http://www.anao.gov.au/WebSite.nsf/0/6fba4dd883a76d69ca256f93006f6a41?OpenDocument

44. *Numbers on the run: Review of the ANAO audit report No. 37 1998−99 on the management of Tax File Numbers*, Standing Committee on Economics, Finance and Public Administration,
<http://www.aph.gov.au/house/committee/efpa/TFNaudit/report.htm>

45. Medicare smartcard, "Privacy information", Health Insurance Commission (as at 18 Feb 2005)
<http://www.hic.gov.au/yourhealth/our_services/medicare_smartcard.htm>

46. *Smartcard not so smart − AMA*, Australian Medical Association, Media Release, 28 July 2004
<http://www.ama.com.au/web.nsf/doc/WEEN−63BAWA>

47. *Australia Card II debate needed*, Edward Mandla − Australian Computer Society, The Australian IT, 7 Dec 2004
<http://australianit.news.com.au/articles/0,7204,11605034%5E15400%5E%5Enbv%5E,00.html>

48. EFA submission to Queensland Transport re Queensland Smart Card Driver Licence Proposal, 21 November 2003.
<http://www.efa.org.au/Publish/efasubm−qt−nqdl.html>

49. Queensland Transport, New Driver Licence Proposal Consultation Package, October 2003
<http://www.transport.qld.gov.au/new_driver_licence>

50. *Smart Card Designers Clamor For Security Tools*, Junko Yoshida, EE Times, 18 Feb 2004
<http://www.techweb.com/wire/26803875>

51. *Smart cards also open to attack*, Kate Mackenzie, Australian IT, 19 November 2002
<http://www.ee.usyd.edu.au/~rjunee/site.cgi?page=ausitarticle>

52. *Power Analysis Attacks :: A Weakness in Cryptographic Smart Cards and Microprocessors*, Ryan Junee, Thesis, November 2002
<http://www.cs.usyd.edu.au/~ryan/thesis/ryan_dpa.pdf>

53. *Smart Cards and Side−Channel Cryptanalysis*, Ryan Junee, Ruxcon Security Conference, Sydney, April 2003
<http://www.ee.usyd.edu.au/~rjunee/sc_side_channel.pdf>

54. *On a New Way to Read Data from Memory*, David Samyde, Sergei Skorobogatov, Ross Anderson and Jean−Jacques Quisquater, First International IEEE Security in Storage Workshop, USA, 11 December 2002
<http://www.cl.cam.ac.uk/ftp/users/rja14/SISW02.pdf>

55. *Camera flash opens up smart cards*, New Scientist, 13 May 2002
<http://www.newscientist.com/news/news.jsp?id=ns99992273>

56. *Lasers crack the key to smartcard chip secrets*, EE Times, 20 May 2002
<http://www.eetimes.com/sys/news/OEG20020517S0016>

57. *Smart Card Security − Defining 'tamperproof' for portable smart media*, Stefano Zanero, Dipartimento di Elettronica e Informazione, Politecnico di Milano, 2001
<http://securenetwork.it/szanero/scsecurity.pdf>

58. *Tamper Resistance − a Cautionary Note*, Ross Anderson & Markus Kuhn, Cambridge University Computer Laboratory
<http://www.cl.cam.ac.uk/users/rja14/tamper.html>

59. *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*
<http://www.privacyrights.org/ar/RFIDposition.htm>

60. Bills Digest, No. 75 2004–05: Australian Passports Bill 2004, Parliamentary Library, 7 Dec 2004
<http://www.aph.gov.au/library/pubs/bd/2004−05/05bd075.htm>

61. ICAO RF Devices Technical Report
<http://www.icao.int/mrtd/download/documents/Annex%20I%20−%20Contactless%20ICs.pdf>

62. *Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security*, American Civil Liberties Union (ACLU) White Paper, 26 Nov 2004
<http://www.aclu.org/Privacy/Privacy.cfm?ID=17078

63. *Sharp begins shipping IC modules to Australia for e−passports*, Junko Yoshida, Electronic Engineering Times, 26 Oct 2004
<http://www.eetimes.com/showArticle.jhtml?articleID=51200486>

64. *Tests reveal e−passport security flaw*, Junko Yoshida, Electronic Engineering Times, 30 Aug 2004
<http://www.eetimes.com/showArticle.jhtml?articleID=45400010>

65. *Does Big Brother want to watch?*, Bruce Schneier, International Herald Tribune, 4 Oct 2004
<http://www.schneier.com/essay−060.html>

66. *Privacy 'risk' in national ID plan*, James Riley, The Australian IT, 21 Jan 2005
<http://australianit.news.com.au/comment/0,10190,12003945%5E26199%5E%5Enbv%5E15306−15319,00.htm

67. *A question of privacy*, Editorial, Sydney Morning Herald, 25 Nov 2004
<http://smh.com.au/articles/2004/11/24/1101219615198.html>

68. NS v Commissioner, Department of Corrective Services [2004] NSWADT 263 (16 November 2004)
<http://www.austlii.edu.au/cgi−bin/disp.pl/au/cases/nsw/NSWADT/2004/263.html>

69. NSW *Privacy & Personal Information Protection Act 1998*
<http:http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464>

70. See note 43.

71. *Weblining*, BusinessWeek Online, 3 April 2000.
<http://www.businessweek.com/2000/00_14/b3675027.htm>

72. *Privacy Principles − irrelevant to cyberspace?*, Graham Greenleaf, Privacy Law & Policy Reporter (Prospect Publishing), 3 PLPR 114, September 1996.
<http://www2.austlii.edu.au/itlaw/articles/IPPs.html>

73. *Keeping track of voters*, The National Interest, Radio National, 23 Jan 2005
<http://www.abc.net.au/rn/talks/natint/stories/s1257392.htm>
Secret NT Govt dirt file revealed, Rebecca Hewett, Northern Territory News, 16 Feb 2005
<http://www.news.com.au/story/0,10117,12265841−17001,00.html>

74. Names of the relevant organisations can be provided to the Committee on request.

75. See note 17.

76. See note 17.

77. See note 17.

78. OFPC Consultation paper on the draft National Privacy Principle Guidelines, Office of the Federal Privacy Commissioner, May 2001.
<http://www.privacy.gov.au/publications/dnppg.html>

79. *Acer on mat over website blunder*, Andrew Colley, The Australian IT, 8 Feb 2005.
<http://australianit.news.com.au/articles/0,7204,12180169%5E15306%5E%5Enbv%5E,00.html>
Major privacy breach at Acer site, Andrew Colley, The Australian IT, 2 Feb 2005.
<http://australianit.news.com.au/articles/0,7204,12124067%5E15318%5E%5Enbv%5E15306,00.html>

▲ Go to Contents List