Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

30 November 2010

Senator D. Cameron
Chair
Senate Environment and Communications Committee
Parliament House
Canberra ACT 2600

Dear Senator Cameron

Re: Inquiry into the Adequacy of Protections for the Privacy of Australians Online

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF made a Submission to the Inquiry in August (no. 14). This was brief, because it was not clear what aspects of the very broad topic were of greatest interest to the Committee.

In view of the very wide scope of the comments made in other Submissions, the APF has prepared a Supplementary Submission, and requests that the Committee accept it, despite the lateness.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation

Australian Privacy Foundation

Supplementary Submission
to the
Senate Standing Committee on Environment, Communications and the Arts
Inquiry into the Adequacy of Protections for the Privacy of Australians Online

30 November 2010

1. Introduction

This Submission comprises some introductory comments, an outline of threats to online privacy, brief comments on the inadequacies of privacy laws, and active measures necessary to address the threats. To assist in 'drill-down' to greater detail, reference is made to material from sources other than the APF, many of them APF Board members. Those items are indented and in italics.

1.1 The Australian Privacy Foundation

The Australian Privacy Foundation (APF) has been, since its formation in 1987, the primary national association dedicated to protecting the privacy rights of Australians. A brief Backgrounder is attached.

The APF has found it necessary to be active on Internet privacy matters on many occasions in the past. Its many Submissions are indexed at:
http://www.privacy.org.au/Papers/indexPolicies.html#Internet

> *Many of the APF's Board members have made significant contributions to privacy research and advocacy in their own right, including (in alphabetical order):*
>
> - *Dr Roger Clarke*
> *http://www.rogerclarke.com/DV/*
> - *Chris Connolly*
> *http://www.galexia.com/public/research/*
> - *Dr Juanita Fernando*
> *http://users.monash.edu.au/~juanitaf/papers/*
> - *Prof. Graham Greenleaf*
> *http://www2.austlii.edu.au/%7Egraham/publications.html*
> - *Prof. Katina Michael*
> *http://ro.uow.edu.au/kmichael/*
> - *Prof. Dan Svantesson*
> *http://www.svantesson.org/publications.aspx*
> - *Nigel Waters*
> *http://www.pacificprivacy.com.au/Papers.htm*

The APF made a brief Submission to the Inquiry in August 2010 (no. 14), focussing on:

(1) privacy and young people

(2) privacy infringements by individuals

(3) consent

(4) cross-border data transfers

Judging by the Submissions as a whole, the Committee is considering the whole breadth of the matter, rather than restricting its focus to specific aspects. The APF has accordingly prepared this Supplementary Submission.

1.2 The Term 'Online'

The APF interprets the term 'online' as used in the Inquiry's title as encompassing Internet activities and other non-voice services using network-connected devices such as 'smartphones' and handhelds, e.g. SMS messaging and ringtone downloads.

However, this Submission focuses primarily on Internet activities.

1.3 Privacy

Privacy is a fundamental human value, of enormous importance in civilised societies, and recognised in international instruments and increasingly in national constitutions as being a fundamental human right. Many aspects of privacy conflict with other interests at economic, social and psychological levels. The process of privacy protection accordingly involves balance among interests.

Too many government agencies and corporations, on the other hand, regard privacy as an inconvenience and an impediment. They seek power over individuals, and work to invade the privacy of individuals and to reduce privacy protections. They commonly do so behind closed doors, avoiding the justifications they provide being open to public scrutiny, and denying civil society a voice in the development of legislation.

This results in a great many provisions being tabled in the Parliament that are grossly privacy-abusive. The Bills' sponsors hope to get them enacted by the Parliament without their impact being appreciated by the public and broadcast in the media. This is in direct conflict with the current Government's commitment to open government.

Privacy is a crucial element in the development and maintenance of public trust in organisations and their activities. The adoption of eCommerce was greatly slowed by distrust, and eGovernment is facing the same problems. Progress in eHealth has been very limited, and is still being seriously undermined, by organisations' cavalier attitudes to personal data. Senate Committees could play a role in forcing organisations to adopt a much more mature approach to privacy. Regrettably, Senate Committees seldom do so.

1.4 'Privacy is Dead'

During recent years, several CEOs of US corporations have perpetrated a myth that the young are not interested in privacy, but are instead very happy to cede their personal data to those corporations in return for services and self-exposure.

The media have adopted this myth uncritically; but it does not bear scrutiny.

People in every generation take risks in their youth, and become more risk-averse as they get older, and accumulate assets, liabilities, responsibilities and things to hide. Many Gen-Ys (people currently aged 15-30) have suffered as a result of over-exposure through actions by themselves and their 'friends'. Moreover, 'iGens' (people currently aged under 15) are already showing signs of understanding the risks involved in online activities. The reasonable conclusion is the opposite of the CEOs' myth – the currently younger generations will be more privacy-sensitive than their predecessors.

Further detail on this analysis can be found in:

- *http://www.rogerclarke.com/II/iGen.html*
- *http://www.rogerclarke.com/DV/MillGen.html*

2. Online Privacy Threats from the Private Sector

2.1 Introduction

The online world offers an enormous range of services, with potentially very high social and economic value. The APF recognises the benefits, and supports the development and exploitation of online technologies and services. Many of the APF's Board members are active in the development, application and use of online technologies and services.

All technologies and services must, however, be subject to careful evaluation of their privacy impacts, and active measures to avoid or at least ameliorate negative privacy impacts. This Submission, by virtue of the nature of the Inquiry, focusses on the negative impacts of online technologies and services.

There are enormous dangers to privacy inherent in the behaviours of Internet services providers such as consumer eCommerce merchants, social network services such as Facebook, and organisations with highly integrated business lines such as Google. There are also enormous dangers to privacy inherent in current copyright laws.

The following sub-sections provide brief outlines of some prominent areas of concern. Unfortunately, the threats are so numerous that it is not feasible to be comprehensive.

2.2 Malware, Malbehaviour and Mal-Infrastructure

Miscreants and criminals have long demonstrated aggressive behaviour, in such forms as spam, cookies, viruses, worms, phishing, web-bugs and distributed denial of service (DDOS) attacks.

> *Categories of malbehaviour and malware are addressed here:*
> *http://www.rogerclarke.com/II/MalCat-0909.html*

Consumers and the devices that they depend upon are highly vulnerable to such attacks.

> *The feasibility of consumer device security is addressed in the following article in the Journal of Law, Information and Science (2007):*
> *http://www.rogerclarke.com/II/ConsDevSecy.html*

Of much greater concern than expressly criminal behaviour is the 'mainstreaming' of malware and malbehaviour, by which is meant their adoption by corporations as weapons against consumers.

Corporations use many forms of malware to gain access to personal data, to exploit it for the benefit of the corporation, and to influence personal behaviour. Some such uses might be argued to be consent-based, but in a great many cases the claim is not tenable. Corporations have been permitted to do this by parliaments, despite the nominal protections afforded by cybercrime laws. In some cases, corporations may have been directly assisted by parliaments, for example by criminalising the reverse-engineering of malware in order to understand its design and devise countermeasures.

Corporations have subverted the architecture and infrastructure of Internet services generally and the Web in particular, in order to provide themselves with greater capacity to breach the security of consumer devices and invade consumers' privacy. Important examples include the following:

- **web-bugs (or 'beacons')** are used to collect information about consumers' behaviour in relation to both email-messages and web-pages, not merely without consent, and not merely without knowledge by the consumer, but with active contrivance by the marketer
- **Microsoft's ActiveX mechanism** creates vulnerabilities within consumer devices by enabling software to operate on the device in a manner that cannot be controlled by the device's user

- outside the Microsoft environment, additional threats (although not as serious as is the case with ActiveX) have been created through new features and techniques commonly referred to as **AJAX** (an acronym derived from 'Asynchronous JavaScript and XML')
- **the Firefox web-browser** was, in its early versions, far more privacy-protective than Microsoft's Internet Explorer. From **version 3.5 onwards**, however, it is more marketer-friendly and less consumer-friendly by virtue of its support for privacy-invasive programming
- **the Flash add-on software for web-browsers**, which is currently the most common means of supporting both video and animation, includes spyware functions that actively but surreptitiously breach consumer privacy, and that have been actively designed to resist countermeasures by people who want to protect themselves

  A resource-page on Flash cookies ('Local Shared Objects') is here:
  http://epic.org/privacy/cookies/flash.html
- **new forms of cookies** have been developed recently. These are even more difficult to detect and to manage than the original forms of cookie, and at this stage it appears they may be impossible to eradicate. Once again, this technology is being implemented non-consensually, and with active attempts to avoid consumers even being aware of it

  A September 2010 article examined the 'evercookie':
  http://arstechnica.com/web/news/2010/09/evercookie-escalates-the-zombie-cookie-war-by-raising-awareness.ars
- **the emergent new standard HTML5** may moderate some of the negative impacts of AJAX and Flash, but in the process it may further empower developers and enable intrusions into data and into the behaviour of consumer devices and of consumers themselves

  An article identifying some of the concerns about HTML5 appeared in the New York Times of 10 October 2010:
  http://www.nytimes.com/2010/10/11/business/media/11privacy.html?_r=2&hp

These features are part of the **'Web 2.0'** movement. This is commonly depicted as being developed in order to provide exciting consumer experiences. In fact, the movement was instigated by marketers, for marketers, and is manipulative and invasive of consumers' data and behaviour.

Web 2.0 is examined in this article in the Journal of Theoretical and Applied Electronic Commerce Research (2008):
http://www.rogerclarke.com/EC/Web2C.html

These capabilities underpin several further developments during the last 5-10 years, which are addressed in the following sub-sections.

2.3 Geo-Location

It is increasingly feasible to detect the location of a device in physical space, through inferences based variously on:

- the IP-address (although such inferences are commonly highly unreliable)
- location within a phone or Wifi cell
- self-reported GPS coordinates

Where this is informed and consensual, it can provide a basis for location-based services. In many circumstances, however, service providers are contriving to gain access without informed consent. Google's Wifi breaches and HTML5 features are part of this field of play.

Moreover, the location of a handset may provide means of inferring the location of a person. This may give rise to serious threats to privacy, including the physical safety of the person concerned.

These articles from 2007 and 2008 address privacy issues in geo-location:
http://works.bepress.com/kmichael/30/
http://www.rogerclarke.com/DV/YAWYB-CWP.html

2.4 Social Networking Services

Social networking services (SNS) were criticised at the time they emerged, because of the risks that they create for personal data.

> *An early analysis from 2004 is here:*
> *http://www.rogerclarke.com/DV/ContactPITs.html*

Many individuals have suffered variously from ill-advised self-exposure, from exposure by 'friends', and from exposure as a result of malperformance and breaches by SNS operators.

Facebook has been particularly blatant in its wholesale disregard for consumer privacy. The company has acted, and continues to act, with both arrogance and with great confidence that US regulators will do very little to protect consumers' privacy and to constrain Facebook's business model.

> *A summary of Facebook's privacy-hostile behaviour during its short life from 2007-10 is at:*
> *http://www.rogerclarke.com/DV/PrivCorp.html#FB*

The business models of SNS are generally based on advertising revenue generated from the acquisition and retention of consumers' attention. Consumers' attention depends in turn on 'compelling' content. The interests of SNS operators are therefore well-served by voyeurism, self-exposure and exposure of other people. This can be encouraged in ways that might be argued to result in consensual disclosures of personal data. On the other hand, SNS operators, and especially Facebook, have frequently utilised devious and even downright fraudulent behaviour to achieve non-consensual exposure, through liberal rather than conservative defaults, obscurity of settings, manipulation of settings, re-definition of settings and re-purposing of data.

There is speculation that personal data, and particularly email-addresses, may be leaking from Facebook, quite possibly via or to its Russian associates Kontakt.ru and mail.ru.

Google's release of the Buzz extension to Gmail adopted a similar approach to Facebook's.

> *Outlines of Google's bad behaviour when it released Buzz are at:*
> *http://www.rogerclarke.com/II/GB-100211.html*
> *http://www.rogerclarke.com/DV/PrivCorp.html#Goo10*

2.5 Behavioural Targeting

The effectiveness of advertising can be enhanced by selecting appropriate advertisements to project to particular consumers at particular times. Marketers claim that this is a service to consumers, as well as a more economically efficient way to promote goods and services. There may well be widespread support for this argument where the consumer is informed, and participates consensually.

In practice, most behavioural targeting is performed without even the consumers' knowledge let alone consent, uses personal data that has been collected surreptitiously, involves the collation of personal data from multiple sources, and involves the correlation of a consumer's identities that arise in different contexts. These all represent gross abuses of privacy, but they have to date been countenanced by parliaments.

> *This October 2010 article documented data trading underlying targeting:*
> *http://www.smh.com.au/technology/technology-news/inside-the-cookie-monster--trading-your-online-data-for-profits-20101004-164ee.html?skin=text-only*
>
> *This 2009 article finds that "Americans Reject Tailored Advertising and Three Activities that Enable It":*
> *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214*

A recently-emerged technique is browser fingerprinting, referred to by marketers as 'clientless device identification' (CDI). This exploits the technical information provided by the consumer's web-browser to the web-server – especially which browser, which browser-version, which operating system, and which fonts are installed – in order to establish a unique fingerprint that is associated with that browser. This fingerprint can then be used as an identifier for the consumer, and can be readily correlated with other identifiers.

> *Browser fingerprinting is addressed in a July 2010 paper by Australian Peter Eckersley, who is on the staff of the US Electronic Frontier Foundation (EFF), at: https://panopticlick.eff.org/browser-uniqueness.pdf*

2.6 Google's Business Model and Behaviour

Privacy invasion is entirely central to Google Inc.'s business. The media promotes on Google's behalf the myth that "'do no evil' is the corporate motto". In fact, the company's strategy has been based since at least 2005 on the principle that 'Google knows a lot about you'.

The frequent anti-privacy comments made by the company's CEO, Eric Schmidt, need to be seen in the the light of the company's profitability being best served by a public perception that privacy doesn't matter any more. That has assisted in the ongoing refusal by parliamentarians to subject the company's behaviour to privacy-protective regulation, and the failure by regulatory agencies to undertake meaningful enforcement actions.

Google has been frequently approached by privacy advocacy organisations in an endeavour to achieve a dialogue, but the company has steadfastly avoided engagement. In Australia, the APF has spent 3 years communicating with the corporation, in an endeavour to convey the need for its behaviour to be substantially changed. The company has failed to respond in a constructive manner.

A recent letter from the APF to Google Australia about the consequences of Google's failure to engage with privacy advocacy organisations is here:
http://www.privacy.org.au/Papers/Google-100827.html

The specific forms of engagement that the APF has proposed to Google are:

(1) advance notice of releases that may give rise to privacy concerns (whether justified or not);

(2) consultation about intended services and features, sufficiently in advance of their release that discussions between the company and privacy advocacy organisations can influence the design.

Even worse than the company's avoidance behaviours are its actively misleading pretence that it acts morally, and its intentional breaches of consumer privacy. For example, the company misled both the APF and every Privacy Commissioner it dealt with in 2008-09 by failing to disclose the monitoring of Wifi networks as part of its StreetView project, despite ample opportunity to be honest.

Beyond that, the manner in which the monitoring of Wifi networks was done breached data protection laws, and was a *prima facie* breach of the Telecommunications (Interception and Access) Act. The very slow handling of the matter by the AFP is consistent with the interpretation that the first legal opinion the AFP acquired suggested the need to proceed to prosecution, and hence a second is being sought in an endeavour to find a way to avoid enforcing the law.

The APF's Policy Statement in relation to Google StreetView is here:
http://www.privacy.org.au/Papers/StreetView.html

The succession of actions by the APF in relation to Google's Wifi breaches are indexed here:
http://www.privacy.org.au/Papers/indexPolicies.html#Internet

> *This 2006 article analysed the challenges Google poses, including to privacy: http://www.rogerclarke.com/II/Gurgle0604.html*

2.7 Cloud Computing

Outsourcing of services brings with it additional risks to personal data. Individuals are unable to exercise any form of control over outsourcers because they are not a party to the contract. Australian privacy law still fails to impose effective regulation on outsourcing.

Conventional outsourcing involves a known organisation storing data in a known location. There is a current fashion of 'cloud computing' or 'cloud-sourcing'. Under these arrangements, the organisation responsible for the data does not (and indeed cannot) know the locations in which the data is stored, processed and backed-up. Because many of the facilities are outside Australia, there is a high likelihood of yet more personal data about Australians leaking out to jurisdictions that do not have adequate data protection laws and enforcement.

Current privacy law is extremely permissive of transborder data flows, because corporations make acceptance of transfer of data overseas a condition of dealing and hence make consent irrelevant. Corporations have been permitted to circumvent privacy law by shifting the data off-shore, and hence online consumers have lost their nominal privacy protections.

The APF's Policy Statement on Cloud Computing is here:
http://www.privacy.org.au/Papers/CloudComp-0911.html

Over a year after the APF's statement that "Regulatory agencies must take proactive steps to investigate and assess the security and privacy risks of using cloud computing, and to educate the public about these risks", no substantiive information is evident on the Privacy Commissioner's site.

> *A 2010 conference paper on user requirements for cloud computing is here:*
> *http://www.rogerclarke.com/II/CCBR.html*

2.8 The Powers Granted to Copyright-Owning Corporations

Until very recently, copyright law balanced the interests of copyright owners and users of copyright works. A range of large corporations have felt threatened by the digital era. Rather than adapting to the changing environment, they have sought and gained protection by the US Congress. Worse still, they have caused successive US Administrations to work for the implementation of these corporate protectionism worldwide. The Australian Parliament has prioritised friendship with the USA over Australian consumers' interests, by passing laws that have massively shifted the balance in copyright laws in order to assist foreign corporations.

Consumers' online privacy is directly undermined by the capacity of corporations to make inadequately justified claims for takedown of works and for access to subscriber identities. The situation is greatly worsened by the Parliament having extended the protection of overseas corporations to the extent of criminalising what had hitherto been civil wrongs, and transferring the costs of enforcement from the aggrieved corporations to the public purse.

The recently signed Anti-Counterfeiting Trade Agreement (ACTA) treaty was negotiated without the transparency, scrutiny or civil society participation. It appears likely to further distort the balance against online consumers and towards the interests of litigants.

3. Online Privacy Threats from the Public Sector

A considerable number of serious threats to online privacy arise in public sector contexts. The following sub-sections identify a small number of them.

3.1 National Security Extremism

Following the terrorist strikes in New York and Washington in 2001, Madrid in 2004 and London in 2005, the Australian Parliament has enacted some 40 statutes that have granted enormous powers to national security agencies. In passing these laws, the Parliament:

- failed its responsibility to ensure that justification for each specific measure was demonstrated rather than being merely asserted
- failed its responsibility to heed the overwhelming opposition of not merely all human rights and privacy advocacy organisations, but also the vast majority of legal professional organisations
- failed its responsibility to impose effective controls over the extreme powers it granted

> *An authoritative summary of the extremist laws is here:*
> *http://www.aph.gov.au/library/intguide/law/terrorism.htm*

The APF's submissions relating to national security extremism are indexed here:
http://www.privacy.org.au/Papers/indexPolicies.html#CT

Subsequent Parliaments have failed to rescind these laws, and hence they continue to constitute massive inroads into human rights, and grave undermining of free society.

There is a current, inexcusable attempt by the Attorney-General's Department, in the form of the TIISL statute, to leak those powers out into the more general law enforcement community.

The APF's Submissions in relation to the TIISL legislation are here:
http://www.privacy.org.au/Papers/Sen-TIISL-101028.pdf
http://www.privacy.org.au/Papers/Sen-TIISL-Supp-101109.pdf
http://www.privacy.org.au/Papers/Sen-TIISL-Hansard-101111.pdf
http://www.privacy.org.au/Papers/Sen-TIISL-Answer-101114.pdf

TIISL was considered by the Senate Legal and Constitutional Committee (SLAC).

> *The Senate Committee Inquiry is here:*
> *http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/index.htm*

> *The Senate Committee's Report is here:*
> *http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/report/report.pdf*

Once again, a Senate Committee abjectly failed in its responsibilities to test proposals put before it on behalf of the national security community. In the face of the unanimous submissions of civil society that the Bill represents an extraordinarily serious and wholly unjustified threat to freedoms, the Committee simply gave the Bill its blessing.

Such inadequate, even fawning behaviour by Senate Committees places in increasing doubt the preparedness of civil society to expend its resources preparing submissions to Senate Committees and making time available to provide verbal evidence.

3.2 The Data Retention Proposals

In April 2010, the Government announced its intention to accede to the European Convention on Cybercrime. This was done without consultation with civil society, and without adequate consideration of personal data security and privacy risks. Even the US baulked at aspects of the Convention, and Canada has adopted a much more sceptical view.

The Attorney-General's Department has been developing a proposal that would greatly extend the regime for data retention by ISPs. Civil society has again been excluded from discussions, and even denied access to documentation.

The matter is addressed in the EFA's Submission to this Committee (no. 20).

On the basis of the limited information publicly available, the proposal, if it is once again rubber-stamped by the Senate Committee, the Senate and the Parliament, will create yet more gross threats to online privacy.

3.3 Censorship / Filtering

Among other potential threats are the Government's long-running and highly ill-advised censorship proposals.

These would be completely ineffective in blocking the kinds of material that they nominally target. On the other hand, there would be serious collateral damage, including to privacy, particularly from the log-files that would be generated.

3.4 The NBN

The Government's proposed temporary control of the Internet backbone and distribution network in Australia via the NBN creates concern that attempts may be made to embed surveillance infrastructure into the network.

It is vital that the Parliament require the NBN project to be submitted to policy examination.

> *This paper from December 2009 identified a range of policy issues, and expressed concern about NBN Co's refusal to consider them and to engage with civil society:*
> *http://www.rogerclarke.com/II/NBN-PC-0912.html*

4. The Adequacy of Privacy Laws

4.1 The Adequacy of Australian Privacy Laws

Existing privacy laws are demonstrably inadequate even for the threats that existed in the 1970s. They are simply no match for the enormously increased threats that exist in 2010.

> *Here is an annotated index of 50 papers on online privacy issues published between 1996 and 2001, a version of which was submitted to the Senate Select Committee on Information Technologies' Inquiry into e-Privacy, of July 2000: http://www.rogerclarke.com/DV/AnnBibleP.html*
>
> *Here is a summary of the ways in which data protection laws of the 'Fair Information Practices' (FIPs) kind, based on the 1980 OECD Guidelines, are even more inadequate in the 21st century than they had been 30 years earlier: http://www.rogerclarke.com/DV/PP21C.html*

4.2 The Adequacy If Projected Changes Are Made

At present, there is a serious risk that, rather than the Parliament enacting substantial increases in privacy protections, it will shortly further undermine the existing, seriously inadequate protections.

The APEC privacy framework was an active attempt by the USA to create an extremely weak alternative to the prevalent European model. The Australian Attorney-General's Department connived with the USA to assist the APEC framework into existence. If any aspects of that empty model were to be implemented in Australia, there would be a massive reduction in protections.

> *An assessment of the APEC framework is here: http://www.austlii.edu.au/au/journals/ALRS/2009/17.html*

The ALRC Report of 2008 recommended the merger of the public and private sector principles into Unified Privacy Principles (UPPs). The Government has submitted draft Australian Privacy Principles (APPs), which are currently before the Senate Finance and Public Administration Committee.

> *Senate Finance and Public Administration Committee*
> *Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation*
> *http://www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm*

The APF expressed very serious concerns in its Submission to that Inquiry, which is here: http://www.privacy.org.au/Papers/Sen-APPs-100818.pdf

> *The APF drew heavily on the analysis conducted by the Cyberspace Law & Policy Centre at UNSW, which is here:*
> *https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=9b3bffed-935d-4ea7-8a8a-123433c9eaec*
> *https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=026c7176-b8d1-4445-9e96-df5cbf05752f*

This initiative threatens massive reductions in privacy protections for Australians. The reasons are as follows:

- details of the Exposure Draft have not been negotiated with a body that includes representatives of all interested parties. Instead, the detailed drafting strongly reflects interests of government agencies, and of business, but excludes civil society from the process; and it consequently contains many privacy-hostile features
- Privacy Principles may be the centrepiece of the proposed legislation, but they are far from the whole story. It is not feasible to conduct analysis and form a reliable opinion, when only part of the draft legislation is made available

- the existing privacy laws are grossly undermined by the raft of exemptions and exceptions. The Exposure Draft not only sustains the existing exemptions and exceptions, but also extends the list, in accordance with special pleadings made by various agencies and industry groups behind closed doors and without the involvement of civil society
- far from enhancing privacy, the new Principles further weaken privacy protections. This applies in particular to Collection (3), Use and Disclosure (6), Cross-Border Disclosure (8), and Government Identifiers (9). All of these contain very serious reductions in the existing legal protections, which should not be passed by the Parliament
- the Exposure Draft entrenches even further the power of the direct marketing industry over consumers. It fails to create obligations, sanctions and enforcement mechanisms. Worse, it elevates Direct Marketing to a 'Privacy Principle' (APP 7) – a corruption of the notion of privacy law that deserves, and would inevitably result in, even more public cynicism about both the purpose of so-called 'privacy law' and the power of the industry over the Parliament
- both federal government agencies and industry associations are pleading their cases for no strengthening of protections, and are doing so behind closed doors, without privacy advocacy organisations being invited into discussions. The inevitable effect is to ratchet each Principle down to the lower of the two standards.
- yet worse, there are about seven other sets of legislated Principles in State and Territory legislation, and each State and Territory is also pressuring for the APPs to accommodate their special pleadings as well, again without any involvement being permitted by privacy advocacy organisations. This greatly exacerbates the 'ratchetting-down' effect
- the already very weak Trans-Border Data Transfer provisions would be watered down to very little at all if the current draft were enacted. This is directly relevant to the present Inquiry, because so much personal data about Australians haemorrhages out to databases overseas

5. Measures Needed

This section identifies measures that need to be the subject of Recommendations by the Committee if this Inquiry is to be part of the solution to online privacy rather than just another part of the problem.

(1) Genuine Privacy Laws in Replacement for the Privacy Act

There is an urgent need for genuine privacy laws that embody privacy protections rather than authorise yet more privacy invasions, that create offences, that apply sanctions and that embody a genuine enforcement regime.

(2) A Genuine Trans-Border Data Protection Law

Serious concerns exist about personal data being permitted to go off-shore. This applies particularly to data held by government agencies, much of which was collected under compulsion of law. However, serious concerns also exist in relation to data held by the private sector, particularly in health and financial services contexts.

The current and proposed transborder provisions need to be abandoned. Organisations should not be given an invitation to 'look the other way' – which is what a 'reasonable belief' test represents. Organisations must remain strictly liable for any adverse consequences, nomatter where the data they are responsible for is located.

(3) Protected Pseudonymity as the Norm

Across both the public and private sectors, there is a very disturbing trend towards increasing demands for people to reveal their identities as part of online transactions. This is based to a considerable extent on the pretences that the only alternative to identification is anonymity and that anonymity creates unacceptable difficulties in making people accountable for their actions.

The concept of protected pseudonymity needs to be much more mainstream in discussions about information infrastructure, applications design and public policy.

(4) Recognition of the Sensitivity of Identity and Location

Identifiers create dangers of data correlation and of identity fraud. Location data creates scope for threats to personal safety, particularly stalking.

Appreciation of the sensitivity of personal data of these kinds needs to be much more mainstream in discussions about information infrastructure, applications design and public policy.

(5) PIAs as Standard Practice in Business and Government

The Privacy Commissioner's Submission (no. 16) recommended that social networking sites be "encouraged" to carry out Privacy Impact Assessments (PIAs) (para. 76). The Privacy Commissioner also merely "suggested" that a PIA be conducted by organisations considering the use of cloud computing (para. 107). And it "supports the use" of PIAs more generally (para. 108).

The Privacy Commissioner's recommendations are appallingly weak. When a matter reaches any Senate Committee, that Committee should expect, and indeed demand, that a PIA has already been conducted, that as part of the PIA consultations have already been held with affected categories of people and their advocates, and that the PIA Report has already been published.

The importance of PIAs being the mainstream, and the default, extends beyond the public sector, especially in online contexts. For example, Google has failed to respond to many submissions by civil society that the company should engage with privacy advocacy organisations. On the sole occasion that Google engaged with the APF in advance, in relation to the original StreetView service, the APF

was able to draw attention to a long list of concerns. During the weeks following the service's release, many of these problems were identified by the public and the media. The company had to scramble to deal with the fallout, when an early PIA and consultations would have enabled them to plan in appropriate privacy protections.

It was noteworthy that the Google submission to this Inquiry (no. 6) made no mention at all of privacy impact assessment, nor of consultation with privacy advocacy organisations.

The Privacy Commissioner should have pilloried the company for failing to undertake PIAs on its projects, and for failing to engage with civil society. The then Privacy Commissioner ignored that opportunity. Instead, the tone of her media release indicated active support for a company that had breached the Privacy Act, rather than support for online consumers.

(6) Effective, Efficient and Privacy-Positive Complaints-Handling

As discussed in ACCAN's submission to the Inquiry (no. 11), there is an urgent need for the new Privacy Commissioner to adopt a much more positive and privacy-protective approach to complaints-handling.

The APF's experience during the regime of the previous Privacy Commissioner was quite appalling, with very slow handling, and every effort made to avoid supporting the public and even to avoid conducting investigations.

(7) An Active, Privacy-Protective Stance by the New Privacy Commissioner and OAIC

The Appendix provides an analysis of the seven functions of the Privacy Commissioner that relate not merely to the narrow area of data protection but to the broad field of privacy protection.

Successive Privacy Commissioners have failed to fulfil these obligations.

Privacy Commissioners in other countries have adopted positive stances. For example, the Canadian Privacy Commissioner led the actions against Facebook's serial breaches, and the German Data Protection Commissioners exposed Google's Wifi breaches. The immediate past Australian Commissioner, on the other hand, went so far as to refuse to join her peers around the world when they jointly wrote to Google regarding their concerns about the manner in which that corporation has designed and conducts its business.

There is an urgent need for a much more active and privacy-protective stance by the new Privacy Commissioner and OAIC, in a manner that reflects those statutory functions.

Senate Committees need to pressure the new Privacy Commissioner to change the mind-set of the organisation from that of a protector of government agencies and business to what the Parliament instructed the Office to be – a protector of people's privacy.

Appendix: The Scope of the Privacy Commissioner's Functions

Privacy comprises multiple dimensions. One analysis distinguishes privacy of the person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data.

Most of the Privacy Commissioner's functions are specifically limited to the privacy of personal data. (This is by virtue of them being expressly defined in terms of the IPPs and NPPs, or indirectly defined in terms of the IPPs and NPPs, in particular through the use of the terms 'privacy code' and 'interference with privacy' – which is defined in ss.13 and 13A in terms of the IPPs and NPPs).

Such constraints apply to 17 of the 24 functions defined in s.27(1). However, the other seven of the Commissioner's functions under that sub-section – copy below – are expressed in terms of privacy. Because the key term 'privacy' is not defined, its usual, broad meaning needs to be applied. Those seven functions therefore empower and require the Commissioner to consider all dimensions of the privacy of individuals, not merely the privacy of personal data. Those functions are:

- the examination of proposed enactments (b)
- research into IT (c)
- the provision of advice (f)
- the examination of proposals for data matching or data linkage (k)
- educational programs (m)
- reports and recommendations (r)
- anything incidental or conducive to those six functions (s)

Commissioners have largely avoided the exercise of the seven functions beyond the narrow realm of the two sets of Privacy Principles. That has been to the serious detriment of privacy protection.

s.27 - Functions of Commissioner in relation to interferences with privacy
http://www.austlii.edu.au/au/legis/cth/consol%5fact/pa1988108/s27.html

(1)(b) to examine (with or without a request from a Minister) a proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals and to ensure that any adverse effects of such proposed enactment on **the privacy of individuals** are minimised;

(1)(c) to undertake research into, and to monitor developments in, data processing and computer technology (including datamatching and datalinkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;

(1)(f) to provide (on request or on the Commissioner's own initiative) advice to a Minister, agency or organisation on any matter relevant to the operation of this Act;

(1)(k) to examine (with or without a request from a Minister) a proposal for data matching or data linkage that may involve an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals and to ensure that any adverse effects of such proposal on **the privacy of individuals** are minimised;

(1)(m) for the purpose of promoting the protection of individual privacy, to undertake educational programs on the Commissioner's own behalf or in cooperation with other persons or authorities acting on behalf of the Commissioner;

(1)(r) may, and if requested to do so, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of individuals;

(1)(s) to do anything incidental or conducive to the performance of any ... other functions.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/