Senate Standing Committee on Environment, Communications and the Arts

Submission to the Inquiry into 'The Adequacy of Protections for the Privacy of Australians Online'

by

Rodney Serkowski

on behalf of

Pirate Party Australia

Table of Contents

Foreword

First and foremost, we welcome and would like to thank the Committee for the opportunity to present these submissions. Pirate Party Australia[1] is a forming political party that focuses on the freedom and access of information, knowledge and culture, and advocates for the protection of civil liberties, especially the protection of privacy.

We hope that sharing our perspective and reflection on privacy in this submission assists the Committee in their task of assessing the adequacy of privacy protections within the Australian legal framework, and any legislative initiatives the government may embark upon in future, that may affect the privacy of Australian citizens.

Preliminary Issues

Whilst the framework of the inquiry concerns itself with the adequacy of current protections 'online', we feel it necessary to contextualise what privacy actually is, how we believe Australians perceive both privacy, and the expectations of law in protecting that privacy in our initial remarks. We believe this will allow the committee to better understand our perspective, and hopefully assist the Committee in their deliberation.

What is Privacy?

Privacy itself is a complex concept that involves different, but intrinsically linked and overlapping individual and personal interests. In simple terms there are three basic fundamental interests that compose the notion of privacy.

The first is informational privacy — the idea that every person must have control over highly personal information about himself or herself. This of course includes information pertaining to health and medical records, including biometric data and genetic privacy, ethnicity, records of financial transactions and other personally identifiable data such as geographic information.

The second is relational privacy. This is the notion that every individual has the ability to determine with whom they will engage with in personal or intimate relationships. The right to form relationships, personal and political, without the intrusion of surveillance, the right to keep familial relationships private. This underpins the freedom of association.

The third is the privacy in decision-making — the freedom from surveillance and others when making decisions in personal affairs. This of course relates

[1] Pirate Party Australia Inc. was incorporated under the Associations Incorporation Act 1984 (NSW) in November 2009 and at the time of this submission has an application before the Australian Electoral Commission for the purposes of registration.

to the requirement in any liberal and democratic nation for the privacy of communication, and the reasoning for the secret ballot. It is an understanding that has been long held to underpin democracy, and as such has been recognised in numerous international human rights instruments and national constitutions.

Perceptions of Privacy

Australia's constitution, as pragmatic as it is, contains within it very little by way of the protection of human rights.[2] Unlike the national constitutions of many other nations that explicitly denote the protection of the privacy of its citizens, there is no power or responsibility explicitly concerned with privacy conferred upon the federal government within the document. As such the Australian citizens have largely had to rely on common law and international human rights instruments as mechanisms that require the government to enact legislation for the purposes of protecting privacy.

Whilst there have been many legislative moves in recent years to protect the privacy of Australian citizens, at both the State and Federal level, the Parliament has not always respected these rights. This has largely been left to non-governmental organisations and civil society to raise awareness and highlight privacy as an important issue, and to explain repercussions of government policy, and to prevent the enactment of highly invasive policies.[3] So whilst it may seem at times that privacy is a concern of a select few, defeat of such policies and the political conflict, media coverage and public outrage they are generate demonstrates the importance Australians place on privacy.[4]

This is despite Australia being in the fortunate position of never having had to re-establish itself to democratic operation after authoritarian rule, such as is the case in many other nations. In recent years due to perceived internal and external threats to security, a climate of fear has been generated and this has had an unnecessary adverse effect on privacy. Invasive mass surveillance, and data surveillance practices are increasingly used and permitted by

---

[2] This is not to discount the protection that it does offer — both explicitly through the right to vote, the protection against unfair acquisition of property, the right to trial by jury, the protection afforded to the freedom of religion, the protection from discrimination with respect to State of residency, and implicitly through the protection of certain rights as determined by the High Court by the very nature and structure of the constitution which necessitates certain freedoms for the proper function of democracy.

[3] Graham Greenleaf and Nigel Waters, 'NSW to Scrap Privacy Commissioner, Reduce Privacy Protection' (2003) 49 *Privacy Law and Policy Reporter* <http://www.austlii.edu.au/au/journals/PLPR/2003/49.html> at 21 July 2010 In this instance the move by NSW to abolish the Privacy Commissioner was defeated in the NSW Upper House largely due to the campaign of non-governmental organisations (NGOs); This is also similar to the awareness raised by NGOs in the defeat of the then Labor Government 'Australia Card' Policy in 1986-7 and similar defeat in of then Liberal Government 'Access Card' Policy in 2006-7.

[4] Graham Greenleaf 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments – Country Studies – Australia' *European Commission Directorate-General Justice, Freedom and Security* (2010) <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf> at 21 July 2010.

legislation (or lack thereof), with relatively little objection due to a gradual expansion of such technology — the cumulative effects of which are not immediately apparent.[5]

There is also a perception that we are seeing intergenerational shifts in social norms and in the importance younger people are placing on privacy — the advent and widespread use of social media like Facebook,[6] where people may share highly personal data about themselves, is often cited as evidence for a loss of relevance for notions of privacy. Such perspectives are often espoused by the owners of such networks, in what can only be described as self-serving redefinitions of the expectation of privacy in accordance with their business model. In the case of Facebook, this has manifested as expansive evolution in the complexity of the agreement with the end-user,[7] and the way in which Facebook has chosen to increasingly marginalise the privacy of its users,[8] and allowing increasingly more invasive use of user information in their advertising business and by their business partners.

Although there can be no argument that social networking does require some voluntary surrender of privacy to a certain degree, and that one of the most important and valuable aspects of the Internet is the ability for one to maximise their social network, this does necessarily mean that notions or expectations of the privacy and security of personal data has shifted. Rather that they are being besieged by market forces and corporate interest. The quintessential representation of this interest manifested itself in the comments of Eric Schmidt, Google's CEO on the United States broadcaster CNBC making the statement that "[i]f you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Attitudes like this, which are ignorant of legitimate reasons that necessitate privacy and are repugnant to a free society, push the expectation of privacy in a direction that should not be readily accepted.

There is active rejection of such a direction, lending credence to the argument that Internet users value their privacy. When Facebook made changes to their software that subsequently led to the exposure of highly personal data, without user's consent campaigns were immediately launched that denounced

---

[5] *Ibid.*

[6] Facebook, '500 million using Facebook: Zuckerberg' The *Sydney Morning Herald* 22 July 2010 <http://www.smh.com.au/technology/technology-news/500-million-using-facebook-zuckerberg-20100722-10lgs.html> at 21 July, 2010; Meaning one in fourteen people now utilise the social networking site for the purposes of communication and sharing.

[7] Nick Bilton, 'Price of Facebook Privacy? Start Clicking' *The New York Times,* May 12 2010 < http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=1> at July 21 2010; Explains how the Privacy Policy of the social networking site now exceeds the length of the US Constitution with 5,830 words, an interesting representation of this evolution can be also be seen in the infographic; Guilbert Gates 'Facebook Privacy: A Bewildering Tangle of Options' *The New York Times* May 21 2010 <http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html> at July 21 2010.

[8] Kurt Opsahl, 'Facebook's Eroding Privacy Policy: A Timeline' (2010) *Electronic Frontier Foundation Deeplinks Blog* <http://www.eff.org/deeplinks/2010/04/facebook-timeline> at 21 July 2010.

the assault on privacy,[9] its farcical privacy policy and committed to leaving the social networking site.[10]

These campaigns were not crying wolf: this non-consensual exposure of private data has allowed a security researcher[11] to collect the personal details of 100,000,000 Facebook users. The potential for malicious exploitation of such information cannot be overstated.

The proposed development of privacy aware networks[12] attracted large community investment and interest, again displaying that the notion that 'privacy is dead' is patently false — people do value privacy, and that while to some extent the market may be able to provide some protection, strong legislative protections with adequate punitive measures for reckless or negligent contravention are necessary to ensure the fundamental right to privacy is not marginalised.[13]

---

[9] Mark Pesce 'Why I quit Facebook (and you should too)' *The Drum Unleashed* 2 June 2010 <http://www.abc.net.au/unleashed/stories/s2915364.htm> at July 21 2010; Sally Jackson 'Facebook, you've been sent a message…Angry users quit over privacy fears' *The Australian* 31 May 2010 <http://www.theaustralian.com.au/business/media/facebook-youve-been-sent-a-message-angry-users-quit-over-privacy-fears/story-e6frg996-1225873244905> at 21 July 2010.

[10] 'We're Quitting Facebook', <http://www.quitfacebookday.com/> at 21 July 2010.

[11] Daniel Emery, 'Details of 100m Facebook users collected and published' *BBC* 29 July 2010 <http://www.bbc.co.uk/news/technology-10796584> at 29 July 2010.

[12] Daniel Grippi, Maxwell Salzberg, Raphael Sofaer and Ilya Zhitmoriskiy, 'Decentralize the web with Diaspora' *Kickstarter* (New York) <http://www.kickstarter.com/projects/196017994/diaspora-the-personally-controlled-do-it-all-distr>

[13] For instance, the need for punitive sanction where reckless or negligent contraventions of privacy protection occur is evident in the recent Google Street View saga, where the organisation had been shown to have contravened the law, yet no sanction could placed upon the organisation by the Privacy Commissioner; Ry Crozier, 'Google breached Australians' Privacy: Commissioner: Google apologises: "We failed badly here."' *IT News* 9 July 2010 <http://www.itnews.com.au/News/219424,google-breached-australians-privacy-commissioner.aspx> at 21 July 2010.

Data Retention

Last month it was revealed that the Federal Government Attorney-General's Department had been for some time considering the implementation of a legislatively mandated telecommunications data retention regime in Australia[14] and had been approaching Internet Service Providers (ISPs) with respect to the extent to which data could be retained. The compulsory standard to which the Department has signaled it was investigating equivalency with was the European Data Retention Directive.[15]

Due to the opacity of government enquiries,[16] and an as yet incomplete Australian proposal, this submission will concern itself with the possible implementation of a data retention proposal similar to the European model.

The European model which was brought into being after the perception of vulnerability following attacks in New York and Washington in September 2001, the Madrid train bombings in March 2004 and July 2005 London Bombings,[17] represents a shift towards an empowerment of law enforcement, beyond a tolerable level of interference with which citizens should be expected to oblige.[18]

Whilst the populace demand security, and politicians often engage in providing an illusion of security by extension of surveillance powers. Increases in surveillance does not reduce crime.[19] What increased surveillance does do is intrude upon the privacy of innocents. There is no evidence whatsoever that data retention or increased surveillance has had any beneficial effect.

---

[14] Ben Grubb, 'Inside Australia's data retention proposal' *ZDNet* 16 June 2010 <http://www.zdnet.com.au/inside-australia-s-data-retention-proposal-339303862.htm> at July 21 2010.

[15] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications networks and amending Directive 2002/58/EC* [2006] OJ L 105/54

[16] The Attorney General's Department is refusing to release documentation as to what it has asked of ISPs in it's enquiries, citing 'unnecessary debate and could potentially prejudice and impede government decision making' — this is entirely unacceptable for a debate on an issue that potentially will unjustifiably and en masse, invade the privacy of the majority of Australians. The debate on data retention should be open, transparent and evidenced based; Ben Grubb, 'No Minister: 90% of web snoop document censored to stop 'premature unnecessary debate' *The Sydney Morning Herald,* 23 July 2010 <http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html> at 23 July 2010.

[17] In Australia, particular pressure has also come from bombings in Bali in October 2002 and October 2005.

[18] It also curious, that Europe in leading the way with the regulation of transaction logs within the Information Society with the establishment of data privacy regime that limited the collection, processing, retention and access to this information, had then implemented the legislative architecture for mass surveillance, despite significant public opposition and little evidence based justification.

[19] Martin Gill and Angela Spriggs, 'Assessing the impact of CCTV' *Home Office Research Study 292* (2005) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7998&rep=rep1&type=pdf> at 21 July 2010.

Human Rights & Data Retention

As the world progresses towards an information-oriented society an increasing degree of our social interaction occurs via telecommunication networks.

Socially, culturally, economically — we conduct our lives on these networks. We consult our lawyers; perhaps we consult a crisis line[20] or seek assistance from drug-counseling websites. The world economy depends on the Internet; everyday business is conducted over the Internet, with highly sensitive and confidential data being transmitted.

The widespread adoption and use of the Internet raises a relatively unanticipated potential for surveillance — dystopic scenarios of 'Big Brother' increasingly become more probable, due to the relative ease for centralised recording of all content and traffic data on the Internet. The same rhetoric used with the introduction of CCTV surveillance cameras is being used to justify the introduction of data retention, with an equal lack of evidence.

In face of opposition to retention of transmitted content, proponents of data retention laws propose to retain meta data - information about the content being transmitted rather than the content it self. However meta/traffic data is not, and should not be considered to be less invasive than content data, and should be afforded the same legal protections. Meta data may in fact require more stringent legal protection — it can be more effectively processed, and analysed automatically. When combined with other data, specific patterns, can be searched for then sorted to certain criteria, all of which is unachievable with content data — and this can be used to decipher and intrusively deduce a wide variety of information about an individual — analysis can reveal a 'person's political, financial, sexual, religious stance or other interests.'[21] However this analysis is not foolproof, and will lead to erroneous incrimination or suspicion. Fishing expeditions by law enforcement present problems, and there is also the issue that traffic data sometimes cannot be linked to a single individual, in that often affects a number of different users simultaneously.[22]

With data retention laws, the typical understanding of law enforcement takes on a new dimension, and the ability to track citizens far exceeds what we traditionally understand of the powers granted to law enforcement. Access to such a wide variety of data, by law enforcement and government officials, especially in secrecy, can and will be abused. Furthermore, the government in its enthusiasm for surveillance, could not adequately ensure that all data retained would not be at risk to abuse from third parties — either by malicious access to vast databases, or unauthorised misuse of traffic data. Prominent

---

[20] For instance, the NSW Health Department supports a non-profit Rape Crisis Centre; <http://www.nswrapecrisis.com.au/About%20Us.htm> at 21 July 2010.

[21] Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Data Retention with ECHR' *European Law Journal* 11(3) 3 May 2005, 365-375.

[22] *Ibid.*

individuals for instance, or even politicians may be compromised, forced to resign or even blackmailed.

In addition to the issues regarding the invasion of privacy and abuse, there is the issue of cost. Any data retention scheme will have significant costs associated, whilst providing no commercial benefit to the CSP. CSPs must make substantial initial investments in infrastructure, staff and process development with ongoing operational costs, for instance maintenance and staff providing retrieval, verification and advice services to law enforcement — costs which must either be subsidised by the government itself, with marginal costs borne by telecommunication providers or the entire cost of compliance to be borne by telecommunications provider, which inevitably means increased costs for consumers, and significant cost burden on the CSP. If the government does initially sponsor such retention, history does show this situation is only temporary, eventually these costs become recognised as simply part of 'doing business' and costs of compliance — the inevitability of cutting corners with respect to security and integrity would then become a significant concern. After all, this data retained is of no use to CSPs.

It is important here, in determining whether blanket retention is justifiable, to distinguish between different approaches to data retention — that is, the difference between the mass, wide-scale, dragnet retention of data and targeted personal surveillance — surveillance or monitoring of an identified person, for specific reason, sanctioned by judicial warrant.[23]

Whilst the latter (with judicial oversight) is acceptable and necessary for the purpose of pursuing legitimate criminal investigation, the other creates unnecessary suspicion, fear and distrust. This has a 'chilling effect' on public discourse — a threat to open communication, to political activity. It also means that consumers may refrain from participating in legitimate and and lawful discussion and transactions in fear that these transactions may be logged and retained for years, potentially to be used against them. Indiscriminate retention is incompatible with human rights and for this purpose cannot be considered legal or legitimate.

It should be noted that it is an arms race between those who implement surveillance, and those who seek to avoid it. Where active surveillance is prominent, it encourages the use of counter-surveillance technologies and methods to help in retaining anonymity and the privacy of communication — this inevitably makes the job of legitimate law enforcement activity much more difficult and costly. People are already familiar with technologies such as Virtual Private Networks (VPNs), simply using HTTPS, or any protocols that support encryption achieve some of these aims. With IPv6 being deployed in coming years, encryption will become an integral party of Internet traffic.

The question is then, for what purposes can such data be used for by law enforcement, should it be retained. Of course, the prevention and

---

[23] Except for exceptions created within, for instance, the *Telecommunications (Interception Act) 1979* for the domestic Australian Secret Intelligence Organisation (ASIO).

investigation of serious criminal activity are the usual stated purposes of data retention regimes — however what serious criminal activity actually is, can often vary according to perspective. Without doubt, terrorist activity or the distribution of child sex abuse material are serious criminal activities, but will this also include other 'cybercrime'[24] for instance copyright infringement?

The Cybercrime Convention

The debate in Australia surrounding retention of data began in the late 1990s, with the development of the Council of Europe Cybercrime Convention[25] (the 'Convention') — a treaty that although providing with the best of intentions a greater fluidity to cross-border law enforcement and co-operations, has serious flaws that do not adequately protect civil liberties and privacy to counterbalance potential abuses by law enforcement and government, that detracts from these 'good intentions'.

The Convention grants law enforcement agencies power for direct access to entire ISP networks, effectively mandating mass surveillance — eaves dropping, interception of private email and any other communication, with insufficient specification in the way of strict procedural safeguards and limitations. Although this may not be a issue for nations with substantial protections, the agreement is being touted as a global standard, after the UN process to establish an International Cybercrime Treaty that adequately respected the centrality of human rights and the necessary safeguards[26] for any criminal justice system, failed.

There are significant concerns, especially regarding the authorisation and implementation of invasive surveillance regimes [like Carnivore, the FBI 'internet tapping' system,[27] now replaced by NarusInsight and rebranded as a slightly more benign 'Digital Collection System',] which is used for mass surveillance and monitoring of Internet communications in real-time within the US, the use of which was subject to court proceedings, in a class action lawsuit led by the Electronic Frontier Foundation (EFF).[28]

---

[24] For instance in the *Council of Europe Cybercrime Convention* the inclusion of 'copyright infringement' is quite curious — whilst many nations may be a signatory and already have complied with Article 61 of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), nations that may accede to this agreement may not have. Copyright is far from stable, and should not be included within such agreements. It comes as little surprise that groups like the Recording Industry Association of America (RIAA) welcomed the agreement.

[25] *Council of Europe Convention on Cybercrime,* opened for signature 23 November 2001 CETS 185.

[26] In compliance with the *Resolution adopted by the General Assembly on the report of the Third Committee (A/55/593) 55/63 Combating the criminal misuse of information technologies* that "[t]he fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse".

[27] American Civil Liberties Union 'The Seven Reasons Why The Senate Should Reject The International Cybercrime Treaty' 18 December 2003 <http://www.aclu.org/technology-and-liberty/seven-reasons-us-should-reject-international-cybercrime-treaty> at 21 July 2010.

[28] <http://www.eff.org/files/filenode/jewel/jewel.complaint.pdf>

Should a data retention scheme ever be implemented, its expansion will be inevitable. The government cannot guarantee, that should it even implement a system with significant protections, that a subsequent government would not amend these safeguards or expand the scope of data retained. We already see the expansion of the European directive for Internet searching history,[29] how long is it before significantly more draconian measures are demanded, for instance the presentation and recording of identification at telephone booths, Internet cafes and wireless hot spots because the current retention regime is 'incomplete', and may be evaded? To pursue mass surveillance and retention of all telecommunications traffic data is to begin the journey down this path.

Conclusion

The threat to national security is understandable, however this does not make it acceptable for the Australian government to circumvent the democratic process, precluding public consultation and discussion, due to fear of scrutiny and debate. The European Directive continues to pose a significant threat to civil liberties, to consumers and the telecommunications industry. It inevitably increases costs and silences what would otherwise be considered lawful transactions. In essence, the European Directive is invasive, illegitimate, unnecessary and over-reaching - and something that the Australian proposal appears to replicate.

We make this submission in the hope that the Australian Government may understand that there is great public concern for privacy, significant opposition to indiscriminate traffic data retention, and that it is unacceptable that such policies are developed and discussed with little public consultation or evidentiary justification.

---

[29] *Written Declaration 29, Rule 123 of the Rules of Procedure on setting up a European early warning system (EWS) for paedophiles and sex offenders;* Christian Engström, 'Written declaration 29, for data retention of Internet searches' 31 May 2010 <http://christianengstrom.wordpress.com/2010/05/31/written-declaration-29-for-data-retention-of-internet-searches/> at 21 July 2010.