EVERYBODY KNOWS: SNOWDEN'S NSA LEAKS, METADATA AND PRIVACY IMPLICATIONS FOR AUSTRALIA

GENNA CHURCHES*

---

* Charles Darwin Law Student number s205834 — Bachelor of Laws Honours Paper, summer 2013.
Supervisor: Felicity Gerry

EVERYBODY KNOWS

TABLE OF CONTENTS

EVERYBODY KNOWS

The price of freedom is eternal vigilance.[1]

I INTRODUCTION

In 1890, lawyers Warren and Brandeis, wrote an influential paper discussing the support within the common-law for a right to privacy.[2] They considered the many similar protections already afforded by the torts of libel, slander and defamation and their homogenous support of a tort of privacy. They believed the press was overstepping the 'bounds of proprietary and decency',[3] dealing in a prurient trade of gossip, stepping so low as to portray 'details of sexual relations'.[4]

Privacy has not attained the great heights which Warren and Brandeis envisaged — instead the media is hacking phones,[5] corporations are collecting masses of metadata[6] and governmental spy agencies have been accessing and retaining metadata *and* communications of ordinary citizens the world over.[7]

Every detail of life is either retained in some form by governments and/or large corporations or at least accessible without permission or judicial check. Data is collected, analysed and retained, granting unsurpassed insight into the most personal of details and thought. How would Warren and Brandeis[8] have felt in today's transparent world? A world which, with the aid of the

---

[1] This quote has been attributed to many different sources from Thomas Jefferson and Abraham Lincoln through to Leonard Courtney, Wendell Phillips and John Curran, Master of the Rolls in Ireland; see also Robert McClelland, 'The Future of Security' (2007) 3(4) *Original Law Review* 107, quoting, Franco Frattini, European Commissioner responsible for Justice, Freedom and Security, 'Our citizens entrust us with the task of protecting them against crime and terrorist attacks; however, at the same time, they entrust us with safeguarding their fundamental rights.'

[2] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 5(IV) *Harvard Law Review* 193.

[3] Ibid 196.

[4] Ibid.

[5] Leveson LJ, Leveson Inquiry, *The Report into the Culture, Practices and Ethics of the Press*, 29 November 2012 <http://www.levesoninquiry.org.uk/>; Lisa O'Carroll, 'Rebekah Brooks To Begin Her Defence At Phone-Hacking Trial', *The Guardian* (online), <http://www.theguardian.com/uk-news/2014/feb/18/rebekah-brooks-defence-phone-hacking-trial-andy-coulson?CMP=ema_546>.

[6] See, eg, Nina Golgowski, 'How Target Knows When Its Shoppers Are Pregnant – and Figured out a Teen Was before Her Father Did', *The Daily Mail* (online), <http://www.dailymail.co.uk/news/article-2102859/How-Target-knows-shoppers-pregnant--figured-teen-father-did.html#ixzz2uOkwgc3X>.

[7] See, eg, The Guardian, *The NSA Files* <http://www.theguardian.com/world/the-nsa-files>.

[8] Warren and Brandeis, above n 2.

documents released by Edward Snowden,[9] has shown privacy stripped bare — nearly every last shred of dignity and decency has vanished. No longer is there a 'right to be let alone', or a right to be forgotten — it appears everybody does indeed know everything about everyone[10] and the right to have a private life has gone.

This paper will discuss the secret retention of metadata and content, discover whether jurisprudence establishes the privacy of such data, consider the legislative controls of Australian Intelligence Communities ('AIC')[11] and expose the ramifications for democracy under Australia's constitutional monarchy.

[9] Glenn Greenwald, Ewen MacAskill and Laura Poitras, 'Edward Snowden: The Whistle-blower behind the NSA Surveillance Revelations', *The Guardian* (online), 10 June 2013 <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
[10] Leonard Cohen, *Everybody Knows* (I'm Your Man, 1988) — a popular singer and song writer predicted that 'Everybody Knows'; see, eg, Sean Curnyn, 'Everybody Knows (Starting with the NSA)', *The Cinch Review* (online), 13 June 2013 <http://www.cinchreview.com/everybody-knows-starting-with-nsa/10482/>.
[11] Australian Intelligence Communities is a blanket term which covers Australian Security Intelligence Organisation ('ASIO'), Australian Secret Intelligence Service ('ASIS'), Defence Signals Directorate ('DSD') now known as Australian Signals Directorate, Office of National Assessments amongst others.

II ENTER STAGE LEFT — THE SNOWDEN DOCUMENTS

In April 2012, Edward Snowden began copying information whilst working as a National Security Agency ('NSA') contractor.[12] On 20 May 2013, Snowden arrived in Hong Kong with between 9000[13] and 1.7 million[14] secret NSA documents. In conjunction with various journalists, the task of progressively publishing the documents has begun.

A *Validity of Snowden Documents*

Whilst there are still many documents to be published,[15] it is clear there is a culture of systematic surveillance of most, if not *all* people — indiscriminate and largely without judicial or Ministerial approval.[16]

In the 'Draft Report on the US NSA Surveillance Program',[17] the European Parliament found:

> compelling evidence of the existence of far reaching, complex and highly technologically advanced systems designed … to collect, store and analyse communication and location data and

[12] Sean Wilentz, 'Would You Feel Differently about Snowden, Greenwald and Assange If You Knew What They Really Thought?', *New Republic* (online), 19 January 2014 <http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe>; Barton Gellman, 'Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished,' *The Guardian* (online), 24 December 2013 <http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html>.

[13] Spiegel Online International, 'Greenwald: "Explosive" NSA Spying Reports Are Imminent', *Spiegel Online International* (online), 19 July 2013 <http://www.spiegel.de/international/world/journalist-says-explosive-reports-coming-from-snowden-data-a-912034.html>.

[14] Michael Kelley, 'NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them', *Business Insider Australia* (online), 14 December 2013 <http://www.businessinsider.com.au/how-many-docs-did-snowden-take-2013-12>.

[15] Ibid.

[16] AAP, 'US Government Appeals Ruling on NSA Data Program', *SBS* (online), 4 January 2014 <http://www.sbs.com.au/news/article/2014/01/04/us-govt-appeals-ruling-nsa-data-program>; see also *Klayman v Obama* (D DC, Dkt # 13 (No 13-0851), # 10 (No 13-0881, 16 February 2013) Memorandum Opinion 58.

[17] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the US NSA Surveillance Program, Surveillance Bodies in Various Member States and the Impact on EU Citizens of Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*, Doc No 2013/2188 (INI), 8 January 2014 ('*Draft Report on the US NSA Surveillance Program*').

> metadata of all citizens around the world on an unprecedented scale and in an indiscriminate and non-suspicion based manner.[18]

The report describes various NSA programmes conducted in conjunction with European Union member states,[19] granting further validity to the documents. The NSA has also confirmed the existence of some programmes.[20]

B *What Is Collected?*

Due to the secrecy of intelligence programmes, it is impossible to know every detail about what *is* being collected, what *can* be collected and in what circumstances information is collected. The Snowden documents grant an insight into surveillance probably occurring *right now*.

1 *GPS/Location Data*[21]

Blanket Global Positioning System ('GPS') data and location data provided by triangulation of mobile phone signals and registrations at mobile phone towers[22] is being collected at a rate of 5

---

[18] Ibid 16 [1].
[19] Ibid 16 [2].
[20] See, eg, David Kravets, 'Reading between the Lines of Redacted NSA Documents', *Wired* (online), 19 February 2014 <http://www.wired.com/threatlevel/2014/02/nsa-gallery/>; James Ball, 'NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show', *The Guardian* (online), 1 October 2013 <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>.
[21] See, eg, 'How the NSA Is Tracking People Right Now', *The Washington Post* (online), <http://apps.washingtonpost.com/g/page/world/how-the-nsa-is-tracking-people-right-now/634/>; Paul Lewis, 'Snowden Documents Show NSA Gathering 5,000,000,000 Cell Phone Records Daily', *The Guardian* (online), 5 December 2013 <http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden>; Barton Gellman and Ashkan Soltani, 'NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show', *The Washington Post (online),* 5 December 2013 <http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html>; 'NSA Defends Global Cellphone Tracking' *news.com.au* (online), 7 December 2013 <http://www.news.com.au/world/breaking-news/nsa-defends-global-cellphone-tracking/story-e6frfkui-1226777696658>.
[22] 'How the NSA Is Tracking People Right Now', above n 21; see also Sharon Rodrick, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes' (2009) 37 *Federal Law Review* 375, 403-5.

billion records a day from users outside the USA.[23] This enables authorities to track users' movements and to probe movements of other devices which may be in the same vicinity.[24]

2 *Undersea Cables*[25]

Information is tapped from fibre-optic undersea cables with the Defence Signals Directorate ('DSD')[26] implicated in collecting data directly from SEA-ME-WE-3 which carries much of Australia's international telephone and Internet traffic.[27]

3 *Backdoors in Software and Data Retention*[28]

Internet and software corporations[29] have been implicated[30] in granting NSA direct access to their servers, enabling access to email, Internet searches, video and communications networks and social media. This access does not require the consent of the service provider.[31]

Other data collection systems[32] collect 'nearly everything a typical user does on the Internet'[33] including *content* and *metadata*. The NSA released a document which claims[34] it only 'touches'

---

[23] Lewis, above n 21.
[24] Ibid.
[25] Ball, above n 20; Phillip Dorling, 'Australian Spies in Global Deal to Undersea Cables', *Sydney Morning Herald* (online), 29 August 2013 <http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html>; Lewis, above n 21; The Australian undersea cable is known as 'SEA-ME-WE-3'.
[26] Defence Signals Directorate recently renamed Australian Signals Directorate. 'DSD' will be used for consistency throughout this paper.
[27] Lewis, above n 21.
[28] Glenn Greenwald and Ewen McAskill, 'NSA Prism Program Taps In To User Data Of Apple, Google And Others', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>; Dominic Rushe, James Ball, 'Prism Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining>; Will Ockenden, 'Australia Prepared Briefing On US Global Internet Spying Program Prism Before Snowden Revelations' *ABC News* (online), 8 October 2013 <http://www.abc.net.au/news/2013-10-08/australia-prepared-briefing-on-prism-spying-program/5004290>; Lenore Taylor, 'Australians will Be Troubled by Google, Facebook and Our Poor Surveillance by US', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/07/australians-troubled-us-surveillance-google-facebook-apple>.
[29] Including Google, Yahoo, Microsoft, Facebook, Skype and Apple.
[30] Greenwald and McAskill, above n 28.
[31] Ibid.
[32] Such as NSA programmes codenamed 'Xkeyscore' and 'Marina'.

1.6 per cent of daily Internet traffic and 0.025 per cent is actually reviewed. However, when calculated on the percentage of internet traffic relating to communications, rather than the download of music and video, 1.6 per cent becomes particularly revealing. Geoff Jarvis, Professor of Journalism and Internet Commentator said; '[By] very rough, beer soaked napkin numbers, the NSA's 1.6 per cent of net traffic would be half the communication on the Internet. That is one helluva lot of "touching".'[35]

4 *Data Sharing*

The 'Five Eyes Agreement' includes the UK, Canada, Australia and New Zealand[36] and instructs the DSD will 'collaborate directly', 'exchange raw material, technical material and end products' in conducting allocated tasks.[37]

The DSD is able to:[38]

> Share bulk, unselected, unminimised metadata as long as there is no intent to target an Australian National — *unintentional collection is not viewed as a significant issue*. However, if a 'pattern of life' search did detect an Australian then there would be a need to contact DSD and ask them to obtain a Ministerial warrant to continue.

This evidences the DSDs' collection of 'bulk, unselected, unminimised metadata' on Australian nationals, information which is so detailed that a 'pattern of life' search can be conducted.[39]

---

[33] 'XKeyscore Presentation from 2008 – Read in Full', *The Guardian* (online), 31 July 2013 <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>.
[34] 'Marina' programme.
[35] Ball, above n 20.
[36] Paul Farrell, 'History of Five Eyes — Explainer', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>.
[37] Ibid.
[38] Ewen McAskill, James Ball and Katherine Murphy, 'Revealed: Australian Spy Agency Offered to Share Data about Ordinary Citizens', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens> (emphasis added).
[39] A 'pattern of life' search constructs a portrait of the individuals' daily activities.

The DSD appears prepared to share retained medical, legal, religious or restricted business information[40] with other members.[41] Further, the document reveals AIC were considering information sharing with non-intelligence agencies,[42] meaning any level of the executive could access such information without a warrant.

5 *Worse to come?*

Defence Minister David Johnston was questioned[43] as to whether there was 'worse to come':

> we must assume the worst. There is no alternative for us now. The 'Five Eyes' have achieved quite amazing and wonderful things in recent generational history and as I said to the Secretary for the Defence and the Secretary of State we have invested far too much in this space to even contemplate a backward step[44]

The American Civil Liberties Union ('ACLU') has brought several actions in District Courts across America[45] and the President has attempted to alleviate public concern over the collection of US data.[46]

However, Australia's response has been typically minimalistic. Greens Senator Scott Ludlam explains:

---

[40] Normally protected by *Privacy Act 1988* (Cth) ('*PA*').
[41] McAskill, Ball and Murphy, above n 38.
[42] Ibid.
[43] At an audience of defence industry representatives at a closed conference in Perth, Western Australia.
[44] Nick Buckley, 'More Spy Leaks to Come: Minister', *The West Australian* (online), 3 December 2013 <http://au.news.yahoo.com/thewest/latest/a/20119934/more-spy-leaks-to-come-minister/>; Katherine Murphy, 'Australia's Surveillance Has "Achieved Too Much" to Stop, Says David Johnson', *The Guardian* (online), 3 December 2013 <http://www.theguardian.com/world/2013/dec/03/australias-surveillance-achieved-too-much-to-stop-david-johnston/print>.
[45] See, eg, *Klayman v Obama,* (D DC, Dkt # 13 (No 13-0851), # 10 (No 13-0881, 16 February 2013) Memorandum Opinion 58.
[46] Spencer Ackerman, 'NSA Statement Does Not Deny Spying On Members Of Congress', *The Guardian* (online), 5 January 2014 <http://www.theguardian.com/world/2014/jan/03/nsa-asked-spying-congress-bernie-sanders> — Politicians such as Vermont Senator Bernie Sanders have been vocal in criticizing surveillance of American citizens.

> The Australian government has tried to be completely opaque about this, our Attorney-General … will just wave their hands and say 'national security', and that is meant to make you stop asking questions.'[47]

A statement released by Timothy Pilgrim, Privacy Commissioner, epitomised the Government's responses to surveillance claims:

> The right to privacy is not absolute — it must be balanced against other important rights and ideals, such as freedom of expression and national security. In Australia, the Federal ... laws recognise this and include a number of exemptions and exceptions for intelligence and law enforcement agencies.[48]

The trend is for national security to ride roughshod over privacy, despite a distinct lack of legislative power for AIC to undertake blanket surveillance of Australians.

6 *Summary*

It is likely, if not certain, AIC are involved in the blanket collection and dissemination of at *least* metadata, if not content of email and text messages, and are likely to have at *least* considered sharing restricted information with other members of 'Five Eyes'.

[47] Ockenden, above n 28.
[48] Bernard Keane, 'Australia's Supine Reaction to Our Surveillance Planet', *Crikey* (online), 14 June 2013 <http://www.crikey.com.au/2013/06/14/australias-supine-reaction-to-our-surveillance-planet/>.

III METADATA

Contrary to comments by Prime Minister Tony Abbott that it is 'essentially the billing data',[49] metadata, can be sensitive and personal information and 'can actually be more revealing than content'.[50]

A *Why is it important?*

Metadata is used by intelligence services to conduct 'pattern of life' searches which map out an individual's daily routine and tasks.[51] The European Parliament commented that it:

> condemns in the strongest possible terms the vast, systematic, blanket collection of the personal data of innocent people, often comprising intimate personal information: emphasises that the systems of mass, indiscriminate surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens[52]

Whilst there is no actual *content* involved, metadata shows *absolutely everything else*, from the subject line of an email[53] through to the search term of a Google search.[54] It shows the senders' and receivers' email addresses, the times and dates of those communications, the webpages visited, the IP address, call data, text message data and the location of the devices[55] and the duration of calls. It shows the usage of social media, and their origins.[56]

---

[49] Oliver Laughland, 'Metadata: Is It Simply "Billing Data", or Something More Personal?', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/metadata-should-it-be-dismissed-as-billing-data-or-is-it-personal-material>.
[50] Ann Cavoukian, Information and Privacy Commissioner, Ontario Canada, *A Primer on Metadata: Separating Fact from Fiction'* July 2013 <http://www.privacybydesign.ca/index.php/paper/a-primer-on-metadata-separating-fact-from-fiction/>.
[51] Ball, above n 20.
[52] *Draft Report on the US NSA Surveillance Program*, above n 17, 17 [9].
[53] Cf, Rodrick above n 22, 391–2.
[54] Ibid 393–5.
[55] *Telecommunications Act 1997* (Cth) s 275A ('*TA*').
[56] See, eg, Laughland, above n 49; Cavoukian, above n 50.

The information which can be gleaned from 'raw' metadata is limitless. Everything from shoe size, location and personal thoughts and persuasions can be deciphered.[57]

The adage 'knowledge is power'[58] immediately springs to mind. However, just how many Australians are creating metadata?

B *Mobile Communications*

Smartphones, the current pinnacle of technology, have combed mediums and technologies which were previously contained within separate devices and far less portable.[59] However, just as this joyous combination has become the 'must have' device for modern life, equally it has become the 'must have' device for modern surveillance.[60]

Smartphone uptake in Australia has been rapid — in 2012, 51 per cent of Australians owned a smartphone.[61] Saturation of all mobile phone users, including conventional mobile phones, has reached 92 per cent of adult Australians.

---

[57] See, eg, Australian Law Reform Commission, *For Your Information: Australian Privacy and Law Practice*, Report No 108 (2008); Cavoukian, above n 50.

[58] Attributed to Sir Francis Bacon although, interestingly the Latin equivalent is the motto of the US program 'Total Information Awareness' — *Scientia est potentia*; see, eg, John Horgan, 'US Never Really Ended Creepy "Total Information Awareness" Programme', *Scientific American* (online), 7 June 2013 <http://blogs.scientificamerican.com/cross-check/2013/06/07/u-s-never-really-ended-creepy-total-information-awareness-program/>.

[59] Emails, satellite navigation, phone calls, cameras, MP3 players, diaries are all functions which have been combined into the smartphone — small and readily portable.

[60] See, eg, Greenwald and McAskill, above n 28; see also Ubiquitous Computing — International Telecommunications Union, *The Internet of Things* (2005) <http://www.itu.int/osg/spu/publications/internetofthings/> — examples of this in everyday life with Wi-Fi capabilities of fridges, through to the logging of smartphones by advertising rubbish bins in the UK which then provided tailored advertising to the device owner and similar systems where devices are logged by traffic lights in Australia. See eg, 'City of London Corporation Wants "Spy Bins" Ditched', *The Guardian* (online), 13 August 2013 <http://www.theguardian.com/world/2013/aug/12/city-london-corporation-spy-bins>; Australian Broadcasting Corporation, 'In Google We Trust', *Four Corners*, 10 September 2013 <http://www.abc.net.au/4corners/stories/2013/09/09/3842009.htm>.

[61] Australian Communications and Media Authority, *Communications Report 2011–12 Series, Report 3— Smartphones and tablets Take-up and use in Australia* (2013) 1.

C *Internet Usage*

Figures from 2012 demonstrate 93 per cent of Australians had accessed the Internet. Further, 80 per cent of Australians had an Internet connection at home, and 32 per cent accessed the Internet via their mobile handset.[62]

Statistics show that whilst users believe the Internet had improved their daily lives, [63] they were concerned about government[64] and corporations accessing their information.[65]

Users believe they should be free to criticise their government and have a right to express their opinion, even if the ideas are extreme.[66] Users also accessed government policy, contacted MPs and government bodies online.[67]

81.3 per cent of users check their email daily[68] and nearly 40 per cent worried about the privacy of such communications.[69]

D *Summary*

These statistics demonstrate Australians, like others throughout the world, rely on the Internet for dissemination of information, social and business interaction and communication in general. Australians utilise the Internet for political communications[70] and believe the Internet should be

---

[62] Australian Communications and Media Authority, *Communications Report 2011–12 Series, Report 2—Australia's Progress in the Digital Economy, Participation, Trust and Confidence* (2012) 4.
[63] Scott Ewing and Julian Thomas, ARC Centre of Excellence for Creative Industries and Innovation, *CCi Digital Futures 2010 the Internet in Australia* (2010) 1-11.
[64] Ibid 41.
[65] Ibid 47-8.
[66] Ibid 41.
[67] Ibid 37-43.
[68] Ibid 14.
[69] Ibid 41.
[70] See generally Theresa Sauter and Axel Burns, ARC Centre of Excellence for Creative Industries and Innovation, *Social Media In The Media: How Australian Media Perceive Social Media As Political Tools* (2013); Jim McNamara and Gail Kenning, 'E Electioneering 2010: Trends In Social Media And Use In Australian Political Communication' (2011) 139 *Media International Australia* 7, 13.

a place where they can freely criticise the government and express opinion and ideas. The secret watching, collecting and analysing such usage *is* a breach of privacy.

IV ENTER STAGE RIGHT — PRIVACY

Privacy has been defined, throughout the years, as many different things. Perhaps it is this confusion over its exact meaning which has, effectively, banished privacy to the realms of legal obscurity. The right to privacy is often propounded as something which *might* protect us from unscrupulous media reports,[71] which *might* protect us from the prying eyes of corporations. It *might* be bound in the common law,[72] it *might* be bound in the *Universal Declaration of Human Rights* ('*UDHR*').[73] Alternatively, there are those academics who believe in reductionism — that privacy is superfluous, that the right to property,[74] liberty and life form adequate protections.[75] However, with respect to electronic surveillance, what does privacy mean?

A *A Right to Privacy — A Right to Property, Liberty and Life?*

Privacy seems such a simple concept — 'the state of being private; retirement or seclusion, secrecy,'[76] 'the interest of a person in sheltering his or her life from unwarranted interference or public scrutiny'.[77] In reality, privacy is a jumble of limited protections which lay in tort,[78] property[79] and a raft of other legal areas,[80] which *may* protect specific aspects of privacy.

1 *Warren and Brandeis*

---

[71] Warren and Brandeis, above n 2; *Doe v Australian Broadcasting Corporation* [2007] VCC 281.
[72] Warren and Brandeis, above n 2; Cf Greg Taylor, 'Why Is There No Common Law Right of Privacy?' (2000) 26(2) *Monash University Law Review* 235.
[73] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948); *International Covenant on Economic, Social and Cultural Rights*, opened for signature 16 December 1966, 993 UNTS 171 (entered into force 3 November 1976) ('*IPPCR*'); *Privacy Act 1988* (Cth) ('*PA*').
[74] Torts such as nuisance and trespass.
[75] See, eg, Amy Peikoff, 'Beyond Reductionism: Reconsidering the Right to Privacy' (2008) 3(1) *New York University Journal of Law & Liberty* 1.
[76] Susan Butler (ed), *Macquarie Concise Dictionary* (Macquarie, 5th edition, 2010) 999.
[77] Peter Butt, David Hamer (eds), *Concise Australian Legal Dictionary* (LexisNexis, 4th ed, 2011) 458.
[78] *American Law Institute, Restatement (Second) of Torts* (1976) SEC 652C.
[79] Intellectual Property Law.
[80] Such as Constitutional protections, and similar legislation to the *Surveillance Devices Act 1998* (WA) etc.

'The right to be let alone', although not strictly coined by Warren and Brandeis, has become reputably linked with their article 'The Right to Privacy'[81]. They explore the evolution of common law and, in particular, tort, from its earliest beginnings where it only afforded a protection to 'a right to life' — a natural extension being a right to liberty, such as freedom from incarceration, and the right to security of property.[82] Once people have security over property and freedom from arbitrary incarceration, quality of life becomes the next fundamental right — the protection of their 'feelings and intellect'.[83] Progressions such as the tort of assault, arising from battery, demonstrate the law's movement from physical actions to protection of the psyche.

Quality of life is protected by torts such as nuisance, which protecting the 'quiet enjoyment' of property from interference. Protection of reputation is granted through libel, slander and defamation further demonstrating the law considers these rights, although largely intangible, worthy of protection. Warren and Brandeis compare the mental harm caused by the unauthorised display of private lives in printed newspapers, with the harms caused by slander and libel:

> The intensity and complexity of life, attendant upon advancing civilisation, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by a bodily injury.[84]

Libel and slander relate to the damage of reputation, whereas harm caused by invasion of privacy needs to encompass the impact on the 'estimate of himself'[85]— the personal feelings damaged.[86]

---

[81] Warren and Brandeis, above n 2.
[82] Ibid 193.
[83] Ibid.
[84] Ibid 196.
[85] Ibid 197.
[86] Ibid.

Instead of stretching libel and slander to fit the right of privacy,[87] the common law protects privacy through the absolute right to control publication of what is private. When one party receives a letter, does the receipt of that letter entitle the receiver to publish the letter? Or does access to a diary grant the accessee the right to publish? *Prince Albert v Strange*[88] held if private letters, which made personal disclosures, were written to particular persons, the Court would rightly issue an injunction to restrain publication, protecting the writer from anguish.[89]

In *Wyatt v Wilson*,[90] Lord Cottenham concluded a man 'is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his,'[91] reflecting 'if one of the late King's physicians have kept a diary of what he heard and saw, the Court would not, in the King's lifetime, have committed him to print and publish it'.[92]

Akin to the right not to be assaulted, imprisoned or maliciously prosecuted, the right of privacy is concluded as partly being a right to control the act of publication, not the protection of private property but one of 'inviolate personality'.[93] Warren and Brandeis predicted this right would not only protect the written word from invasion but also the individual from the press, photographers, or 'the possessor of any other modern device for recording or reproducing scenes or sounds'[94] with particular emphasis on protecting domestic life from exploitation.[95]

They focused on the right of solitude, the right to have some sanctity in one's home. This theory was successful in *Griswold v Connecticut*,[96] where laws ordering disclosure of information

---

[87] In 1960, Prosser developed this theory further, concluding that there are four torts which make up privacy. These were subsequently published in *American Law Institute, Restatement (Second) of Torts* (1976) SEC 652C; William Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383.
[88] (1849) 49 ER 1302.
[89] Ibid 202.
[90] (1820) unreported.
[91] Warren and Brandeis, above n 2, 205.
[92] Ibid.
[93] Ibid 206, 212.
[94] Ibid 206.
[95] Danielle Keates Citron and David Gray, 'Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards' (2003) 126 *Harvard Law Review Forum* 262, 269–70.
[96] 381 US 479 (1965).

regarding birth control use by married couples were held invalid, breaching the right of marital privacy.[97]

(a) Brandeis J

Brandeis became Justice Brandeis of the United States Supreme Court and was influential in many of the early *United States Constitution* Amend IV ('*Fourth Amendment*') search/privacy cases. In *Olmstead v United States*,[98] he prophetically commented:

> in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. *Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.* Advances in the psychic and related sciences may bring *means of exploring unexpressed beliefs, thoughts and emotions* … Can it be said that the Constitution affords no protection against such invasions of individual liberty?[99]

(b) Roe v Wade[100]

This case was based on the 'penumbras' doctrine,[101] holding Texan laws forbidding abortions during the first trimester were invalid due to the invasion of privacy. A considerable portion of

[97] Some US jurisprudence until this point had denied the existence of Warren and Brandeis's version of privacy — see, eg, *Roberson v Rochester Folding Box Company*, 64 NY 422 (1902); *Pavesich v New England Life Insurance Co*, 50 SD 68 (1905) — both cases involved the use of the plaintiff's image in advertising against their wishes.
[98] 277 US 438 (1928).
[99] Ibid 474 (Brandeis J) (emphasis added).
[100] 410 US 113 (1973).
[101] Rights based Constitutional interpretation.

the right of privacy can be attributed to the *United States Constitution/Bill of Rights* especially the *Fourth Amendment*.[102]

Analogies have been drawn between the 'penumbras' and the High Court's 'constitutional implications',[103] such as the implied freedom of political communication. However, protections steeped in the common law and various constitutions have not been formulated in recent history. Instead, it is important to analogise the protections afforded with their modern equivalent — mail has become email, telephones are still used, although free from wires. There are other technologies, just as Brandeis J predicted, which have allowed far more perverse ways to intrude on an individual's privacy.[104]

Metadata allows an individual to be tracked wherever they carry their smartphone, the internal contents of emails can be collected and searched without the sender or recipient even becoming aware.[105] Governments have the power to reveal the thoughts and opinions of individuals using Internet searches or electronic communications.[106] However, there is sufficient case law to demonstrate such data is private and deserving of the highest protection.

B *Jurisprudence of Metadata — Building a Fence*

1 *Privacy Cases*[107]

Victoria Park Racing v Taylor ('*Victoria Park*')[108] was long held as a barrier to Warren and Brandeis's common law privacy protections.[109] Although that opinion has been negated by the

---

[102] *Roe v Wade*, 410 US 113 (1973) (Blackmun J).
[103] Rights based interpretation of the *Australian Constitution*; Peter Bailey, *The Human Rights Enterprise in Australia and Internationally* (LexisNexis 2009) 658.
[104] *Olmstead v United States*, 277 US 438,474 (Brandeis J) (1928).
[105] Contrary to a regular search warrant where a copy is given; see also *Warshak v United States*, 490 F 3d 455 (6th Cir, 2007); see also *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*') ss 7, 63, 105 — ISP and carriers are required not to disclose interception and access authorisations.
[106] See, this paper 'Metadata'.
[107] This is by no means an exhaustive list.

High Court in recent years, the case demonstrates the existence of privacy behind closed doors or a 'fence'[110] consistent with US jurisprudence.

(a) Victoria Park

The plaintiff conducted 'competitions in the comparative merits of racehorses'[111] at its Victoria Park Racecourse. Taylor built a platform on his property, obtaining commanding views of the racecourse activities and tote board, and allowed commentary to be broadcast via radio. The plaintiff sought an injunction and brought actions in nuisance and copyright. The High Court ruled against the plaintiff, but the deliberations were pertinent — had the defendant taken the plaintiff's property or, more rightly in the case of privacy, did the plaintiff have a right to privacy in this spectacle?

There was no property in a spectacle[112] — Taylor was free to watch and broadcast horse racing occurring at Victoria Park. Victoria Park Racing had no right to privacy for their races — if viewable outside the racecourse they were not private. Latham CJ opined: 'the law cannot by an injunction in effect *erect fences which the plaintiff is not prepared to provide*. The defendant does no wrong to the plaintiff by looking at what takes place on the plaintiff's land'.[113]

---

[108] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.
[109] See, eg, *Australian Broadcasting Corporation v Lenah Game Meats Pty* Ltd (2001) 208 CLR 199, 249 (Gummow and Hayne JJ) 277-8 (Kirby).
[110] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 494 (Latham CJ).
[111] Ibid, 502 (Rich J); it is arguably correct to say that an action in nuisance may have protected a private individual property owner or indeed a business (save a corporation) from the prying eye of a neighbour and, today, statutory provisions such as the *Surveillance Devices Act 1998* (WA) may have offered some protection should spying be sufficiently serious, the mental distress caused by such actions may have been protected by *Khorasandjian v Bush* (1993) QB 727, 742–4 and the developing tort of privacy as enunciated in *Grosse v Purvis* (2003) QDC 151. However, it must be kept in mind that holding race meets was a public event, to which the public paid any entry fee. Also, there were steps that Victoria Park Racing could have taken, such as moving the tote board from the view of Taylor and erecting a screen to block the view of Taylor's platform. The discussions on what privacy is *not*, maybe sufficient jurisprudence to demonstrate that metadata should be protected.
[112] *Australian Broadcasting Corporation v Lenah Game Meats Pty* Ltd (2001) 208 CLR 199, 321 (Callanan J) — considered it time to recognise property in a spectacle.
[113] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 494 (Latham CJ) (emphasis added).

If the spectacle is viewable or visible to third parties, there is no right to privacy. The same sentiment is expressed in historical cases such as *Entick v Carrington*,[114] where the court held: 'the eye cannot by the laws of England be guilty of a trespass'.[115]

Kevin Gray[116] used the analogy of a lighthouse. If the lighthouse keeper chooses to turn on the light, he cannot discriminate between vessels which see the light and those which do not — the light is non-excludable. However, that does not deny the keeper his right to control the light or 'spectacle', a concept important when considering privacy of data which is created — is metadata non-excludable property?

Metadata, *required* by service providers to facilitate communications, is protected by the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*'),[117] preventing disclosure of such information unless requested by a law enforcement or the Australian Security Intelligence Organisation ('ASIO') who has obtained the relevant authority.[118] Therefore, the law has ensured *excludability*. With this in mind, *Victoria Park* supports the notion that metadata is private — it is not viewable by third parties and the law has effectively 'erected a fence'.[119]

It would not be unreasonable to categorise metadata as property. The bundle of rights[120] associated with property have been satisfied — the right to exclude others,[121] the right to use and enjoy the property,[122] the right to possess, and the right to alienate.[123]

---

[114] (1765) 95 ER 807.
[115] Ibid, also quoted in *Kyllo v United States*, 190 F 3d 1041 (9th Cir, 1999) ('*Kyllo*').
[116] Kevin Gray, 'Property into Thin Air' (1991) 50(2) *Cambridge Law Journal* 252, 269.
[117] *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*').
[118] Ibid s 175(2).
[119] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 494 (Latham CJ).
[120] CA Arnold, 'The Reconstitution of Property: Property As a Web of Interests' (2002) 26 *Harvard Environmental Law* Review 281, 283.
[121] TW Merrill, 'Property and the Right to Exclude' (1998) 77 *Nebraska Law Review* 730, 731 — through the Telecommunications (Interception and Access) Act 1979 (Cth).
[122] By creating metadata by using electronic communications.
[123] Samantha Hepburn, *Australian Property Law Cases Materials and Analysis* (LexisNexis Butterworths, 2nd ed, 2012) 37–8.

(b) Katz v United States ('Katz')[124]

Katz had been transmitting wagering information across state lines from a number of phone booths, violating federal law. The FBI installed listening devices in two of the phone booths, without a warrant. The phone booths were made of glass with a closable door. Precedent had established that protection under the *Fourth Amendment* required 'that a person have exhibited an actual (subjective) expectation of privacy and second that the expectation be one that society is prepared to recognise as reasonable'.[125] The Court held:

> [That Katz] was not [seeking privacy from] the intruding eye — *it was the uninvited ear*. He did not shed his right to do so simply because he made calls from a place where he might be seen… *One who occupies* [a telephone booth], *shuts the door behind him*, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.[126]

The recording devices violated the *Fourth Amendment* due to Katz's subjective expectation of privacy and societal expectations of privacy in a phone booth. Again, the 'erection of a fence' to protect privacy has appeared.[127]

(c) Smith v Maryland ('Smith')[128]

In *Smith*, the Supreme Court held the installation of a 'pen register'[129] on a telephone line without a warrant did not constitute a *Fourth Amendment* violation. Determining factors included the difference between listening into *actual* content as opposed to merely recording the phone numbers of outgoing calls, whether the subscriber had a reasonable belief the numbers

---

[124] *Katz v United States*, 389 US 347 (1967) ('*Katz*').
[125] Ibid 361.
[126] Ibid 352 (emphasis added); see also Kevin Emas and Tamara Pallas, '*United States v Jones*: Does Katz Still Have Nine Lives?' (2012) 24 *St. Thomas Law Review* 116.
[127] The analogy of closing the phone booth to shield from the uninvited ear and erecting a fence to obscure the view of racing in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.
[128] 422 US 735 (1979).
[129] A method of recording the numbers dialled on a telephone.

dialled would be held to be private and another *Katz* principle, something shared with third parties can no longer be held to be private.

If metadata only showed the number dialled, then *Smith* supports of the collection of metadata without a warrant. However, the 'pen register' was installed on a telephone line owned by a specific target, as opposed to the blanket collection. Further, those in dissent held 'it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life'.[130] Sound familiar?[131]

(d) Kyllo v United States ('Kyllo')[132]

In *Kyllo*, the *sanctity of the fence* was considered.[133] Kyllo was suspected of growing marijuana inside his triplex unit. Police used a heat imaging camera to look for heat emitted from marijuana production. The images showed the roof of the garage and one side wall of the home was hot. Kyllo was convicted but sought to have the images suppressed. The Court found the images were non-intrusive and only showed the outside of the home. It 'did not show any people or activity within the walls of the structure' and 'the device used cannot penetrate walls or windows to reveal conversations or human activities',[134] demonstrating the same principle found in *Victoria Park* — if the activity was visible from the street, or outside of the home then it could not be held to be private. A second appeal confirmed: '[No] expectation of privacy because he made no attempt to conceal the heat escaping from his home, and even if he had, there was no objectively reasonable expectation of privacy because the imager "did not expose any intimate details of Kyllo's life"'.[135]

---

[130] *Smith v Maryland*, 422 US 735, 748 (Stuart J dissenting) (1979); David Bender, 'What You Need to Know about NSA Mass Acquisition of Telephony Metadata' (2013) 30 (9) *Computer & Internet Lawyer* 1, 5.
[131] Similar claims are made in this paper, see, this paper, 'Metadata'.
[132] 533 US 27(2001).
[133] Ibid 29.
[134] *United States v Kyllo*, 1996 US 3864, 3–5 (15 March 1996) Affidavit, 190 F 3d 1041 (9th Cir 1999) Reviewed 533 US 27 (2001).
[135] 533 US 27, 31(2001); Emas and Pallas, above n 126, 135.

However, the Supreme Court applied the *Katz* test and found there was a reasonable expectation of privacy in the home which society expected law enforcement to honour. Scalia J noted thermal imaging might 'disclose, for example, at what hour of the night the lady of the house takes her daily sauna and bath — a detail many would consider intimate'.[136] It was the ability to see beyond the fence — beyond the point where people consider themselves to be *in* private.

(e) Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd ('Lenah')[137]

In *Lenah*, surveillance cameras were surreptitiously installed in an abattoir used to kill possums for pet meat.[138] The footage was supplied to the ABC by an animal rights group. Lenah was successful in obtaining an injunction, but, on appeal to the High Court, the majority held the injunction should not have been granted as corporations do not have a right to privacy.

Gleeson CJ observed the difficulty in discerning what is private and what is not private:

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. *The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.*[139]

This is analogous to the *Katz* principles — the expectation of privacy when and where an individual subjectively considers themselves to be in private, and whether society recognises that expectation to be reasonable.

---

[136] Ibid 38; see also Emas and Pallas, above n 126, 136.
[137] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
[138] Ibid 237 [77].
[139] *Australian Broadcasting Corporation v Lenah Game Meats Pty* Ltd (2001) 208 CLR 199, 226 [42] (Gleeson CJ) (emphasis added).

Kirby J raised the issue of freedom of political communication[140] under the *Australian Constitution* and balanced the public interest in the footage, finding it should be released.[141]

Lenah removed *Victoria Park* as the barrier to the evolving tort of privacy — however, it is unnecessary to explore further in this paper.

(f) Warshak v United States ('Warshak')[142]

In 2005, a fraud investigation into Warshak obtained a sealed order from a Magistrate Judge, requiring 'any email communications received by the specified accounts that the owner or user of the accounts has already access, viewed or downloaded'.[143] The ISP was prevented from revealing the contents of the order.[144] Warshak initiated a suit against the United States after the orders were unsealed. The District Court found there is a 'reasonable expectation of privacy in his personal emails' which is not removed when the communication is stored on the server of an ISP.[145] Furthermore, they granted injunctive relief preventing the United States acquiring the contents of emails 'without providing the relevant account holder or subscriber prior notice'.[146] In the Sixth Circuit, the Court agreed,[147] however, the case was reheard *en blanc*,[148] avoiding a ruling on the *Fourth Amendment* issue.[149]

---

[140] Ibid 330-9 (Callanan J) — raised the opposing opinion that to apply the freedom of political communication to the facts of this case would involve a considerable and therefore unacceptable, expansion of it. See, this paper 'Constitutional Rights'.
[141] Ibid 277-83, 286-88 (Kirby J).
[142] 490 F3d 455 (6th Cir. 2007); *Warshak v United States*, (No 1:06-cv-357, 2006) US Dist LEXIS 50076, (SD Ohio 2007).
[143] This is consistent with the *Stored Communications Act* 18 USC § 2703(a) (2000 & Supp 2005); Tamar R Gubins, '*Warshak v United States*: The Katz for Electronic Communication' (2008) 23 *Berkeley Technology Law Journal* 723.
[144] Ibid § 2703(d) — ISP and carriers are required not to disclose under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*') ss 7, 63, 105.
[145] *Warshak v United States*, (No 1:06-cv-357, 2006) US Dist LEXIS 50076, (SD Ohio 2007) 19.
[146] Ibid 32.
[147] *Warshak v United States*, 490 F3d 455 (6th Cir, 2007).
[148] *Warshak v United States*, No 06-4092, 2007 US App LEXIS 23741 (6th Cir 9 October 2007).
[149] Vacated *Warshak v United States*, No 06-4092, 2007 US App LEXIS 23741 (6th Cir 9 October 2007); Gubins, above n 143, 723.

2 GPS Cases[150]

Due to the ability of metadata to reveal the exact location of a person, this data can be analogised to the use of a GPS tracker.

(a) United States v Knotts ('Knotts')[151]

Without a warrant, Police placed a GPS tracker on a barrel of chemicals used to manufacture narcotics and followed the signal from the place of purchase to the place of manufacture. A warrant was then obtained to search the premises. Knotts sought to have the search ruled invalid and suggested if the Court found GPS usage valid, then dragnet surveillance could occur across the country without 'judicial knowledge or supervision'.[152] However, the Court found the usage valid as it was only used for a single trip: 'If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.'[153]

(b) United States v Jones ('Jones') [154]

In *Jones*, a GPS tracker was fitted to Jones's motor vehicle for 28 days without a warrant. Sotomayor J discussed the intrusive nature of such a device as it generates a comprehensive record of an individual's movements. She questioned the 'chill factor'[155] associated with the knowledge the government is watching and highlighted the very real ability of the executive to misuse such a powerful form of surveillance. Similar concerns were raised in *People v*

---

[150] Global Positioning System.
[151] *United States v Knotts*, 460 US 276 (1983).
[152] Ibid 283; Emas and Pallas, above n 126, 133.
[153] Ibid 284; Emas and Pallas, above n 126, 134.
[154] 132 US 945 (2012).
[155] See also Anthony Bendall and Jason Forte, 'The Privacy Impacts of the Proposed Changes to Australia's National Security Regime' (2012) 9(2) *Privacy Law Bulletin* 14, 16.

Weaver,[156] with both cases finding GPS devices breach the *Fourth Amendment* amongst other principles.

(c) United States v Maynard ('Maynard') [157]

Arising from the same fact scenario as *Jones*, the Court in *Maynard* was given the opportunity to answer the pertinent question raised in the case of *Knotts*[158] — was blanket 24-hour surveillance of citizens throughout the country without judicial knowledge or supervision constitutionally sound? The Court responded: 'The police used the GPS device not to track Jones's "movements from one place to another," but to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.'[159]

The court applied the *Katz* principle, considering what Jones had knowingly exposed to the public:

> whether something is exposed to the public as that term was used in *Katz* … what a reasonable person expects another might actually do … We hold the whole of a person's movements over the course of a month is not actually exposed to the public because *the likelihood a stranger would observe all those movements is not just remote, it is essentially nil*.[160]

The Police suggested Jones had 'constructively exposed' those movements, individually, to the public over the entire period. The Court held: 'the whole may be *more* revealing than the parts. Applying the precedent to the circumstances of this case, we hold the information the police discovered using the GPS device was not constructively exposed.'[161]

---

[156] 12 NY 3d 433 (2009); Bender, above n 130, 5.
[157] 615 F 3d 568 (2010).
[158] *United States v Knotts*, 460 US 276 (1983).
[159] *United States v Maynard*, 615 F 3d 568, 609-10 (2010); Emas and Pallas, above n 126, 140-1.
[160] Ibid 560.
[161] Ibid 561 (emphasis added); Emas and Pallas, above n 126, 140.

The Court considered 'mosaic theory' — the GPS tracker may not collect any more information than a 'traditional' surveillance operation, but it is impossible for such traditional methods to be so cheap, comprehensive and limitless in time.[162] With a GPS trackers, the State can acquire every detail of movements, similar to a 'pattern of life' search as conducted by the NSA and AIC. Again, the problem is not the individual 'snippets' of information but the *information as a whole* is so detailed and so limitless that the *whole becomes more revealing than the parts*.

3 *Jurisprudence Summary*

Australian and US jurisprudence establishes something which is done with the expectation of privacy, or something which is done behind closed doors or behind a fence, draws the expectation of privacy. These concepts are analogous with modern technologies as follows:

(a) Metadata

Metadata is produced every time a call, email or internet search is undertaken. Is it an expectation such data will be kept private? Are these activities conducted behind a 'fence'?

The answer to both these questions is a resounding yes. Users take steps to protect the privacy of devices through passwords, firewalls, anti-virus and anti-theft software. Telephone calls are similarly shielded by closing a door or seeking seclusion from the 'uninvited ear' and even public computers are generally contained within a semi-enclosed booth — protection measures which parallel closing the telephone booth in *Katz*, the fence in *Victoria Park*, the images in *Kyllo* and the relevant *expectation* of privacy.[163]

Similarly, the test enunciated in *Lenah* indicates where individuals seek to protect their privacy, and such expectations are not unreasonable, their activities and information should be deemed to be private.

---

[162] Emas and Pallas, above n 126, 141.
[163] See also *Klayman v Obama*, (D DC, Dkt # 13 (No 13-0851), # 10 (No 13-0881, 16 February 2013) Memorandum Opinion 58.

Furthermore, the privacy of such data is recognised in the *TIAA*,[164] demonstrating Parliament's recognition.

(b) Location Data

Whilst individuals' movements outside of their homes are exposed to the public gaze, it is the ability of location data to show the whole picture, which, as demonstrated in *Maynard*, is more revealing than the part.

The ACLU has initiated a suit against the United States government stating: '[collecting metadata] gives the government a comprehensive record of our associations and public movements, revealing a wealth of detail about our familial, political, professional, religious and intimate associations.' [165]

The 'Petraeus scandal' in the US was based on metadata — General David Petraeus, former head of the CIA and his mistress were tracked through their metadata, revealing simultaneous meeting points. Actual content was not required.[166]

There are several Acts which limit the use of GPS trackers, demonstrating Parliament's recognition of need for protections.[167]

C *Human Rights*[168]

The *UDHR*[169] enshrines privacy at art 12: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

---

[164] See, this paper, 'Legislative Power — Mass Metadata Collection'.
[165] *American Civil Liberties Union v Clapper* (D NY No 13 Civ 3994, 11 June, 2013) [1].
[166] Hal Hodson, 'How Metadata Brought Down CIA Boss David Petrous', *The New Scientists* (online), 16 November 2012 <http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html#.UxDQZoW2V5d>.
[167] See, eg, *Surveillance Devices Act 2004* (Cth); *Surveillance Devices Act* 1998 (WA).
[168] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948) ('*UDHR*').

Similar wording is used in the *International Covenant on Civil and Political Rights* (‘*ICCPR*’) art 17.[170] With both treaties ratified, Australia, operating under its dualist system, has enacted *some* domestic legislation to give effect to these treaties.[171]

However, the primary privacy legislation, the *PA*, only regulates the way information collected by *certain* government agencies and organisations is handled and disseminated. This is known as informational privacy which grants *some* protections to medical and government records amongst others.[172]

Legislation to protect citizens from arbitrary surveillance has not been so successful. Whilst there are some provisions in, for instance, the *TIAA*, to ensure law enforcement agencies obtain warrants before the interception of communications,[173] AIC are bound by less stringent requirements.[174]

United Nations High Commissioner, Navi Pillay, commented: ‘People need to be confident that their private communications are not being unduly scrutinised by the State. The right to privacy,

---

[169] Ibid.
[170] *International Covenant On Civil And Political Rights International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, ratified Australia 13 November 1980, 999 UNTS 171 (entered into force 23 March 1976) (‘*IPPCR*’) — article 17 has the addition of the word unlawfully — no one shall be subjected to arbitrary or unlawful interference.
[171] This comment must be qualified by the occasions where the High Court has considers Australia's international obligations under treaties which may not have received adequate domestic legislation to give them domestic force. See, eg, Mabo *v Queensland (*No 2*)* (1992) 175 CLR 1; see also Kirsten Walker, ‘International Law as a Tool of Constitutional Interpretation’ (2001) 28(2) *Monash University Law Review* 86.
[172] D Banisar and Simon Davies, Electronic Privacy Information Centre and Privacy International, *Privacy And Human Rights 2000: An International Survey Of Privacy Law And Developments*, <http://gilc.org/privacy/survey/intro.html> — considers there are several different types of privacy, being informational privacy, bodily privacy which covers genetic testing cavity searches et cetera, privacy of communications which covers email, mail telephones et cetera and territorial privacy which considers the intrusion into personal spaces such as the home or the workplace or public space in general.
[173] *Telecommunications (Interception and Access) Act 1979* (Cth) (‘*TIAA*’) s 39; prohibition s 7.
[174] *Telecommunications (Interception and Access) Act 1979* (Cth) (‘*TIAA*’) — allows for Ministerial approvals rather than warrants for content; other acts such as *Surveillance Devices Act 2004* (Cth); *Surveillance Devices Act* 1998 (WA) have been legislated but exceptions and reduced requirements apply to AIC.

the right to access, to information and freedom of expression are closely linked. The public has the democratic right to take part in the public affairs …'[175]

Various comments by the Human Rights Committee[176] have confirmed the *ICCPR* should be interpreted as guaranteeing rights to privacy against 'state authorities or from natural or legal persons'[177] — unlawful interferences include actions by state authorities which do not comply with the basis of law, and provisions and objectives of the covenant.[178] Further: 'State parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the covenant, and to provide the legislative framework prohibiting such acts by natural or legal persons.'[179] It also states: 'surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wiretapping and recording of conversations should be prohibited.'[180]

Furthermore, where decisions are made to authorise interference, it must be done so under the respective domestic law and on an individual case basis, upholding the confidentiality of communications. Such interference should be balanced with the interests of society, but only insofar as it is *essential* to protect society's interests.[181]

Considering there have been no terrorism prosecutions attributed to the blanket collection of metadata,[182] it is hard to argue such collections are essential to protect society's interests. There

---

[175] Office of the High Commissioner for Human Rights, 'Mass Surveillance: Pillay Urges Respect for Right to Privacy and Protection of Individuals Revealing Human Rights Violations' (Media Release, 2 July 2013) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13534&>.
[176] *CCPR General Comment Number 16: Article 17 (Right To Privacy) The Right to Respect Of Privacy, Family, Home And Correspondence, And Protection Of Honour And Reputation*, 3rd Comm, 32nd Sess (8 April 1988); see also *Draft Resolution — The Right To Privacy In The Digital Age*, 3rd comm, 68th sess, agenda item 69(b), UN Doc A/C.3/68/L.45/Rev.1 (20 November 2013).
[177] *CCPR General Comment Number 16: Article 17 (Right To Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 3rd Comm, 32nd Sess (8 April 1988).
[178] Ibid [3].
[179] Ibid [9].
[180] Ibid [8].
[181] Ibid [7].
[182] See, eg, Melanie Hunter, 'Deputy AG: Governments Meta Data Collection May Have Resulted in One Criminal Case' *CNS News* (online), 4 February 2014 <http://cnsnews.com/news/article/melanie-hunter/deputy-ag-

are no domestic laws which allow for such collection,[183] making collection inconsistent with domestic law and the provisions and objectives of the *ICCPR* and *UDHR*.

government-s-metadata-collection-may-have-resulted-one> — there has been possibly one criminal case which has resulted in the US.

[183] See, this paper, 'Legislative Authority — Mass Metadata Collection'.

V LEGISLATIVE AUTHORITY — MASS METADATA COLLECTION

The *TIAA* and the *Intelligence Services Act* 2001 (Cth) ('*ISA*') both limit the ability to undertake *any* surveillance, let alone blanket surveillance. The *PA* places limitations upon sharing information which has been legally collected but AICs are excluded.

A *Telecommunications (Interception and Access) Act 1979 (Cth) ('TIAA')*

The Explanatory Memorandum to the 2006 Amendment Bill states:

> telecommunications interception and access to stored communications, the Act makes clear that the general position is that these activities are prohibited, except in certain clearly defined situations. This reflects the primary focus of the Act which is to protect the privacy of communications.[184]

The *TIAA*, despite its antiquated language,[185] still restricts the collection of metadata. Metadata is not defined, but is covered under 'telecommunications data'.[186] To access metadata, [187] the *Act* requires an ASIO officer seek authorisation from the Director General of Security, the Deputy Director General of Security or other approved officer.[188] The authorising officer must be satisfied 'that the disclosure would be in connection with the performance by the Organisation of its functions.'[189] Whilst there are a number of broad 'functions' under which to obtain the information,[190] there are *no blanket provisions* which allow ASIO to collect bulk metadata without individual authorisation. Furthermore, authorisations are limited to 90 days.[191]

Similarly, other law enforcement agencies must adhere to an authorisation scheme which requires the authorisation to be 'reasonably necessary' for the enforcement of criminal law or

---

[184] Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth) pt 3-1.
[185] See, eg, Rodrick above n 22.
[186] Ibid 388.
[187] *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*').
[188] Ibid s 175(2).
[189] Ibid s 175(3); for prospective documents s 176(4).
[190] *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIOA*') s 17.
[191] *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*') s 176(5)(b).

protecting revenue.[192] Access to content is more difficult, with interceptions and access to stored communications requiring a warrant issued by the Attorney-General.[193]

Whilst the above provisions effectively allow ASIO to circumvent judicial approvals, the Acts still *seriously limit* the ability to undertake blanket metadata from everyday citizens. Whilst it is possible these agencies may obtain separate authorisation for each and every individual, it would be a time-consuming task, fraught with danger of being caught issuing authorisations without valid reasons.[194]

B *Intelligence Services Act 2001 (Cth) ('ISA')*

The DSD and Australian Secret Intelligence Service (ASIS) conduct their activities under this *Act*. These organisations are primarily tasked with foreign intelligence activities. However, with Ministerial authorisation,[195] they are able to undertake activities to produce intelligence on an Australian, providing the Minister is satisfied the activity is necessary for the proper performance of the function of the agency,[196] the authorisation will not be exceeded[197] and arrangements have been made to ensure the nature and consequences of acts done will be reasonable.[198]

Further, the Minister must be satisfied the Australian person is likely to be involved in activities which range from a threat to security,[199] risks to the person's safety,[200] the proliferation of

[192] Ibid ss 178(3), 179(3); *Telecommunications Act 1997* (Cth) ('*TA*') ss 276, 277.
[193] *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*') ss 9, 109.
[194] Attorney-Generals Department, Australian Government, *Telecommunications (Interception and Access) Act 1979, Annual Report 2012-13* (2013).
[195] *Intelligence Services Act 2001* (Cth) ('*ISA*') ss 8, 9.
[196] Ibid s 9(1)(a).
[197] Ibid s 9(1)(b).
[198] Ibid s 9(1)(c).
[199] Ibid ss 9(1A)(a), (b).
[200] Ibid s 9(1A)(a)(i)

weapons of mass destruction,[201] a serious crime involving money, goods, people,[202] or intellectual property[203] and using electromagnetic energy.[204]

It is unlikely many Australians could be construed to fit the above without some *serious* misinterpretation. There is nothing in this *Act* which authorises blanket collection of metadata on Australian citizens in Australia.

However, something more sinister lurks at s 15.[205] Every Minister responsible for one of the agencies must create a set of written rules regulating the communication and retention of intelligence information concerning Australian people.[206] This must be done in consultation with the Directors of the relevant agencies and the Inspector General of Intelligence and Security ('IGIS') and the Attorney-General. These privacy rules must be consistent with the proper performance of these agencies' duties.

On inspecting the rules for ASIS, r 4 (Communication of Information not deliberately collected) reads:

> 4.1 ASIS may communicate intelligence information concerning an Australian person that was not deliberately collected to an authority that ASIS is permitted to cooperate with, provided the authority has been approved by the Minister for the purpose of this rule.
>
> 4.2 Before approving an authority for the purpose of rule 4.1, the Minister is to be satisfied that there are satisfactory arrangements in place to ensure that the authority will abide by the ASIS privacy rules.[207]

---

[201] Ibid s 9(1A)(a)(iv).
[202] Ibid s 9(1A)(a)(v).
[203] Ibid s 9(1A)(a)(vi).
[204] Ibid s 9(1A)(a)(vii).
[205] Ibid s 15.
[206] Australian Secret Intelligence Service, Australian Government, *Privacy Rules* <http://www.asis.gov.au/Privacy-rules.html>.
[207] Ibid.

Rule 4 in the *DSD Privacy Rules* is identical.[208] Serious questions have to be asked — why would information 'not deliberately collected' be kept? Surely a Ministerial approval under s 9 would not allow for the retention of such data?[209] And why would this, arguably unlawful data, be shared? How could such data be necessary for the proper performance of the agencies' functions? Is *all* data being collected, and targeted individuals' information filtered out, leaving *massive* amounts of information which could technically be deemed 'not deliberately collected'?

Is this the point where it can only be assumed there *is* blanket data collection occurring, with authority for such collections somewhat akin to an iceberg — the majority of which lays hidden from public view, whilst occasional glimpses atop the ocean, such as these Privacy Rules, giving reason to know of its presence?

This is not the first time the DSD and its activities have been brought into question. In 1999, similar surveillance claims were made, codenamed 'Echelon'.[210] In response to such claims, DSD confirmed it is bound by the *TIAA* and classified *Rules on Signit and Australian Persons* which prohibit:

> the deliberate interception of communications between Australians in Australia, the dissemination of information relating to Australian persons gained accidentally… or the reporting or recording of the names of Australian persons mentioned in foreign communications.[211]

---

[208] Defence Signals Directorate, Australian Government, *Privacy Rules*, *Rules to Protect the Privacy of Australians* <http://www.asd.gov.au/publications/dsdbroadcast/20121002-privacy-rules.htm>.
[209] *Intelligence Services Act* 2001 (Cth) ('*ISA*').
[210] Ross Colthart, 'Big Brother Is Listening', *Sunday Program* <http://sgp1.paddington.ninemsn.com.au/sunday/cover_stories/transcript_335.asp>; Inspector General of Intelligence and Security, *Report MV Tampa, August – September 2001 – Collection And Reporting Of Intelligence Relating To Australians* Document Number 20502/02 <http://www.defence.gov.au/minister/13tpl.cfm?CurrentId=1441> — In 2001, accusations of phone tapping of the Maritime Union of Australia and the International Transport Federation were investigated.
[211] Letter from Martin Brandy, Director, Defence Signals Directorate to Ross Colthart, Reporter, *Sunday Program* 16 March 1999 <http://cryptome.org/jya/dsd-sigint.htm>.

Furthermore, the DSD claims that any Australian communications *inadvertently* collected are destroyed, which is clearly contrary to the privacy rules above.[212]

C *Australian Security Intelligence Organisation Act 1979 (Cth) ('ASIOA')*

ASIO's controlling legislation allows the organisation to use GPS tracking devices, but only with approval of the Minister[213] and not for more than 6 months.[214] However, the *TIAA* allows ASIO to obtain authorisation to metadata, which can be used to track an individual, thus circumventing the restrictions imposed under *ASIOA.*

D *Privacy Act 1988 (Cth) ('PA')*

The *PA* contains principles regarding the collection, storage disclosure of personal information by some private organisations[215] and government agencies.[216] Personal information is defined as: 'Information or an opinion… 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.[217]

However, AIC are exempted from this *Act*.[218]

---

[212] Ibid; see also Parliamentary Joint Committee on Intelligence and Security, Parliament of the Commonwealth of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, 139 — report on the proposed 'Data Retention Scheme' further demonstrating a lack of legislative power.
[213] *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIOA*') s 26B; objects s 26C.
[214] Ibid s 26B(5); objects s 26C(5).
[215] *Privacy Act 1988* (Cth) ('*PA*') s 6C.
[216] Ibid s 6(1).
[217] Ibid.
[218] *Privacy Act 1988* (Cth) ('*PA*') ss 7(1)(f), (g); 7(1A); 7(2)(a), (b).

E *Surveillance Devices Acts*[219]

These *Acts* regulate the use of surveillance devices such as GPS trackers on employees[220] and prevent usage by private individuals. In Western Australia, the use of trackers by law enforcement agencies requires a judicial warrant,[221] but applying only to state-based offences.[222] In all other circumstances, the Commonwealth Act applies, allowing the use of trackers without authorisation from approved officers[223] — such restrictions do not apply to AIC.

F *Summary of Legislative Authority*

AIC have vast powers to intercept metadata. Whilst there are legislative protections as to whose data can be collected, the secret nature of such agencies prevents many disclosures. However, it is clear there are *no* provisions for the widespread collection of metadata.[224]

---

[219] See, eg, *Surveillance Devices Act 2004* (Cth); *Surveillance Devices Act* 1998 (WA).
[220] See, eg, *Workplace Surveillance* Act 2005 (NSW) s 16.
[221] *Surveillance Devices Act* 1998 (WA) s 12; save an emergency s 20 — less protections are afforded under the *Surveillance Devices Act 2004* (Cth); see also *R v Giannakopoulos* [2013] SASCFC 50.
[222] See, eg, *R v Giannakopoulos* [2013] SASCFC 50; *Surveillance Devices Act 2004* (Cth) s 7.
[223] *Surveillance Devices Act 2004* (Cth) s 39.
[224] See also *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, above n 212.

VI OTHER LEGAL PROTECTIONS AND PRINCIPLES

A *Legally Privileged Information*

AIC have demonstrated their willingness to share privileged and confidential information.[225] Privilege is vital in conferring trust and candour between lawyer and client, with clients necessarily requiring the ability to give frank disclosure to their lawyer, [226] without fear such disclosures may prejudice their position.[227] Australia has been implicated in spying on US lawyers advising Indonesia in trade talks and disclosing the information to US businesses,[228] raising further concern regarding the liability of lawyers if client confidentiality[229] is breached by AIC.[230]

B *Rule of Law*

> [T]he absolute supremacy or predominance of regular law as opposed to the influence of arbitrary power … means … equality before the law or the equal subjection of all classes to the ordinary law of the land administered by the ordinary courts; the 'rule of law' in this sense excludes the idea of any exemption to officials or others from the duty of obedience to the law which governs other citizens or from the jurisdiction of the ordinary tribunals.[231]

---

[225] McAskill, Ball and Murphy, above n 38.
[226] *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002) 313 CLR 543.
[227] See, eg, *Smith v Jones* [1999] 1 SCR 455; G E Dal Pont, *Lawyers Professional Responsibility* (Lawbook, 5th ed, 2013) 356-409.
[228] See, eg, Birdie Jabour, 'Australia spied on Indonesia talks with US law firm in 2013', *The Guardian* (online), <http://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm>; Martin Pengelly, 'US Law Firm Was Caught in NSA Surveillance Net in Indonesia — Report', *The Guardian* (online), <http://www.theguardian.com/world/2014/feb/15/us-law-firm-nsa-surveillance-indonesia-australia>.
[229] Dal Pont, above n 227, 333-54 — the duty to keep client information confidential is found in contract, equity and professional conduct rules.
[230] Leanne Mezrani, 'Spying Case Raises Questions Of Liability', *Lawyers Weekly* (online), 25 Feburary 2014 <http://www.lawyersweekly.com.au/news/spying-case-raises-concerns-about-law-firm-liabili?utm_source=Cirrus+Media+Newsletters&utm_campaign=21b70018d3-Lawyers+Weekly+Newsletter+-+20140225111724&utm_medium=email&utm_term=0_fe913f1856-21b70018d3-59556813>.
[231] AV Dicey, *Introduction to the Study of the Law of the Constitution* (Macmillan, 6th ed, 1902), 198.

The rule of law protects people from 'arbitrariness, prerogative or even of wide discretionary authority on the part of the government'.[232] However, since the days of AV Dicey, modern governments have grown to where, particularly in the AIC, there is immense executive discretion — arguably one which should lie with the judiciary. The judiciary are required not only as a check on the executive but also to interpret what the law is. 'It is empirically the province and duty of the judicial department to say what the law is'.[233]

Blanket metadata collection can only be described as arbitrary and unauthorised by law, making such actions contrary to the rule of law.

Furthermore, strong argument could be made that the law is not being prescribed equally — that the data of every citizen is being scrutinised by AIC and yet, in the realms of law enforcement, only the data of persons of interest. This double standard favours the person who may be guilty of wrongdoing — they are protected by authorisation to intercept the data.

C *General Warrants*

'[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he tread upon his neighbour's ground, he must justify it by law.'[234]

During the time of King Henry VIII, the printing press allowed publications seen as seditious and non-conformist to be published. Henry introduced a license system regulating the publication of materials, and to tackle 'black market' publications, searches and seizures became commonplace.[235] Many of these searches were undertaken under a warrant termed 'general'. These warrants were identity non-specific — any person at any time could be searched. Agents

---

[232] Ibid 198.
[233] *Marbury v Maddison*, 5 US 137, 177 (1803).
[234] *Entick v Carrington* (1765) 95 ER 807.
[235] Otis Stephens and Richard Glenn, *Unreasonable Searches and Seizures — Rights and Liberties under the Law* (ABC Cilo, 2006), 30.

of the Crown who undertook searches could have been members of designated private entities such as the Stationers Company, the corporate body tasked with regulating the printing system.

Sir Edward Coke[236] was searched as he lay on his deathbed. His residence and law chambers were searched and items such as manuscripts of his legal writings, his valuables and a poem addressed to his children, were seized.[237]

In *Wilkes v Wood*,[238] John Wilkes, a Member of Parliament, printed pamphlets criticising the British government. A general warrant was issued for the search and arrest of the authors and 49 people were arrested over a three day period. Pratt CJ,[239] found the warrant was 'totally subversive of the liberty [and] the person and property of every man in this kingdom'.

Editor of *The Monitor*, John Entick, found himself subjected to a general warrant. In *Entick v Carrington*, Pratt CJ said general warrants allow searches of: 'the secret cabinets and bureaus of every subject in this kingdom … whenever the Secretary of State shall think to charge, or even to suspect, a person to be the author printer or publisher of a seditious libel.'[240]

Similar to the blanket collection of metadata, these warrants were non-specific, removing the requirement of reasonable suspicion.

[236] A great English jurist and writer (1552-1634).
[237] Stephens and Glenn, above n 235, 31.
[238] (1763) 19 Howell's State Trials 1153.
[239] Shortly thereafter elevated to Lord Camden.
[240] *Entick v Carrington* (1765) 95 ER 807, 1063; Stephens and Glenn, above n 235.

D *Constitutional Rights*

In *Nationwide News Pty Ltd v Wills* ('*Nationwide*')[241] and *Australian Capital Television Proprietary Ltd v Commonwealth* ('*ACTV*'),[242] an implied right to the freedom of political communication was found by the High Court within the *Australian Constitution*. In *Nationwide*, it was held provisions in the *Industrial Relations Act 1988* (Cth) relating to criticising the Australian Industrial Relations Commission or a member, were invalid. The majority found such provisions infringed upon freedoms to discuss governments — a process which is vital to the dissemination of information when individuals are preparing to vote — Deane and Toohey JJ lamented:

> The people of the Commonwealth would be unable responsibly to discharge and exercise the powers of governmental control which the Constitution reserves to them *if each person was an island, unable to communicate with any other person*. The actual discharge of the very *function of voting in an election or referendum involves communication* … thesis of the doctrine is that the powers of government belong to, and are derived from, the governed, that is to say, the people of the Commonwealth.[243]

To be able to discharge their responsibility as voters in the doctrine of representative government, individuals need to disseminate information and communicate freely.

In *ACTV*, similar facts were found when the Commonwealth attempted to impose a blanket prohibition on political advertisements on radio or television, except for those parties granted free time. Free time was allocated at the discretion of the Australian Broadcasting Tribunal however, 90 per cent was reserved for parties represented in the previous Parliament. This was

---

[241] (1992) 177 CLR 1.
[242] (1992) 177 CLR 106; see also *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 529; see also *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 280 (Kirby J); Elisia Arcioni, 'Developments in Free Speech Law in Australia: Coleman and Mulholland' (2005) 33 *Federal Law Review* 333; see also Jude McCulloch and Joo-Cheong Tham, 'Secret State, Transparent Subject: The Australian Security Intelligence Organisation in the Age of Terror' (2005) 38(3) *Australian and New Zealand Journal of Criminology* 400.
[243] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1 (Deane and Toohey JJ) (emphasis added).

found to be a breach of the implied freedom of political communication and as such the provisions were invalid. Mason CJ, enunciated a test:

> *Only a compelling justification will warrant the imposition of a burden on free communication by way of restriction and the restriction must be no more than is reasonably necessary to achieve the protection of the competing public interest which is invoked to justify the burden on communication.* Generally speaking, it will be extremely difficult to justify restrictions imposed on free communication which operate by reference to the character of the ideas or information. But, even in these cases, it will be necessary to waive the competing public interests, *though ordinarily paramount weight would be given to the public interest in freedom of communication.* So, in the area of public affairs and political discussion, *restrictions of the relevant kind will ordinarily amounts to an unacceptable form of political censorship.*[244]

The test has been further clarified in the case of *Lange v Australian Broadcasting Corporation*.[245] The two-stage test asks: 'does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect?' If so, is that burden justifiable?[246]

In the case of metadata, statistics have demonstrated Australians feel they should be able to criticise their government online[247] — however, has such a freedom been impaired and is that burden justifiable in the public interest?

The collection of metadata is not proportional to national security or the public interest. The public interest is better served by freedom of political communication than the stifling gaze of Big Brother.[248]

---

[244] *Australian Capital Television Proprietary Ltd v Commonwealth* (1992) 177 CLR 106, 142–3 (Mason CJ) (emphasis added).
[245] (1997) 189 CLR 520.
[246] The second limb of the two-stage test was augmented in *Coleman v Power* (2004) 220 CLR 1, 50 (McHugh J) — 'is the law reasonably appropriate and adapted to serve a legitimate end which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government?'; see Sarah Joseph and Melissa Castan, *Federal Constitutional Law, A Contemporary View* (Lawbook, 3rd ed, 2010) 444-5.
[247] See, this paper, 'Metadata'.

VII WHO IS TO BLAME?

A *The Relevant Minister or AIC?*

The doctrine of responsible government holds the Minister accountable when a department underperforms. In turn, the Minister is responsible to Parliament and ultimately responsible to the voters. However, this doctrine has been rendered somewhat impotent by the majority, two-party nature of Australian politics, and does not effectively open the executive voter scrutiny.[249]

Moreover, *could* a Minister act against the advice of his department when something as important as national security is involved? Or *would* a Minister be *able* to act against a department which had a full set of retained metadata ready to be used as leverage?

B *Office of the Inspector General of Intelligence and Security*

This Department, headed by Dr Vivian Thom, is tasked with overseeing the actions of AIC.[250] Civil Liberties Australia ('CLA') made a written request[251] that Dr Thom undertake an inquiry on surveillance as disclosed by the Snowden documents — she responded it was 'not my department' and 'definitely not my department' in her subsequent response.[252]

Her refusal is concerning as she is *obliged* to take action on such a written request. Where a complaint is received from outside the Minister's Department, there is an obligation to make enquiries where 'Australian citizens or permanent residents are affected or a law of the Commonwealth, a State or a Territory may be violated'.[253]

Further, the 2012/13 report states:

---

[248] George Orwell, *1984*, read online as an e-book <http://gutenberg.net.au/ebooks01/0100021.txt>.
[249] Joseph and Castan, above n 246, 10.
[250] Authorised by *Inspector General of Intelligence and Security Act 1986* (Cth) and *Intelligence Services Act* 2001 (Cth) ('*ISA*') pt 3.
[251] *Inspector General of Intelligence and Security Act 1986* (Cth) s 10.
[252] Bill Rowlings, 'The Public Deserves a Spy Inquiry Now', *New Matilda* (online), 5 December 2013 <https://newmatilda.com/2013/12/05/public-deserves-spy-inquiry-now>.
[253] *Inspector General of Intelligence and Security Act 1986* (Cth) s 8(2); powers of enquiry s 8(4).

> The role of the IGIS … broadly, to assist Ministers in the oversight and review of the legality and propriety of the activities of … (AIC) … ensuring that these activities are consistent with human rights … in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny.[254]

If Dr Thom will not initiate an inquiry then who will?

[254] Inspector General of Intelligence and Security, Australian Government, *Annual Report 2012 – 2013*, 1.

VIII DOES PRIVACY MATTER?

It cannot be said the downfall of privacy was not foretold. In his book, *1984*[255] Orwell predicted a form of surveillance-state type dystopia. Leonard Cohen proposed that *Everybody Knows*[256] and countless others have predicted totalitarian regimes and dystopias where society is constantly surveilled.[257]

Why are these predictions of society always negative? Why do individuals want to escape the tyranny of surveillance?

The answer is disconcerting. To have a truly free society where democracy reigns supreme, individuals must have the right of free thought, the right to disagree with government, the right to have different religious beliefs, the right to have political free speech against the powers that be. The term, 'intellectual privacy', has been coined where individuals have the right to think, read and communicate without surveillance or interference.[258]

Brandeis J commented in the case of *Whitney v California*:[259]

> Those who won our independence believed that the final end of the state was to make a men free to develop their faculties; and that, in its government, the deliberative forces should prevail over the arbitrary. They valued liberty both as an end, and as a means. They believed liberty to be the secret of happiness, and courage to be the secret of liberty. They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth.[260]

---

[255] Orwell, above n 248.
[256] Leonard Cohen, *Everybody Knows* (I'm Your Man, 1988) — a popular singer and song writer.
[257] See, eg, Aldous Huxley, *Brave New World*, read online as an e-book <http://www.huxley.net/bnw/one.html>; Alexander Linklater, 'The Circle, by Dave Eggers — Book Review', *The Guardian* (online), 13 October 2013 <http://www.theguardian.com/books/2013/oct/12/the-circle-dave-eggers-review>.
[258] Neil M Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934, 1935.
[259] 274 US 357, 375 (1927).
[260] *Whitney v California*, 274 US 357, 375-6 (Brandeis J) (1927).

Freedom of thought is essential to a free and democratic society. Consider *Australian Communist Party v Commonwealth,*[261] where the High Court held invalid the *Communist Party Dissolution Act 1951* (Cth). Whilst the *Act* was struck down for being ultra vires, freedom of association and freedom of political communication were protected. Kirby J later commented:

> lawyers and citizens in Australia have looked back with appreciation and gratitude to this Court's enlightened majority decision in the *Communist Party* case. Truly, it was a judicial outcome worthy of a 'free and confident society' which does not bow the head at every law that diminishes liberty beyond the constitutional design … In the face of contemporary dangers from terrorism, it is essential that this Court should insist on the steady observance of settled constitutional principles. … It should reject legal and constitutional exceptionalism. Unless this Court does so, it abrogates the vital role assigned to it by the Constitution and expected of it by the people. That truly would deliver to terrorist's successes that their own acts could never secure in Australia.[262]

Jeremy Bentham conceived the idea of the 'Panopticon',[263] a prison where a surveillance tower granted the warden vision into each of the cells. Bentham explained: 'to be incessantly under the eyes of an inspector is to lose in fact the power of doing ill, and almost the very wish'.[264] Unable to predict when or if they were being watched was sufficient to change prisoners' behaviours to conform to the Warden's ideals.

1984 depicts overzealous children seeking out 'thought-criminals', the constant fear of being watched and its *conforming* influence:[265]

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. *It was even conceivable that they watched everybody all the time*. But at any rate they could plug in your wire whenever they wanted to. *You have to live — did live, from habit*

---

[261] (1951) 83 CLR 1.
[262] *Thomas v Mowbray* (2007) 233 CLR 307, 433 [387]-[388] (Kirby J).
[263] Jeremy Bentham, 'Panopticon of Bentham' in Basil Montagu (ed), *Three Opinions Of Different Authors Of Upon The Punishment Of Death* (1813), 321.
[264] Ibid, Richards, above n 258.
[265] Orwell, above n 248.

> *that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.*[266]

Similarly, the Chinese Government is denigrated over Internet censorship and surveillance of citizens.[267]

Ramifications such as 'selective prosecutions' and blackmail demonstrate the perverse nature of the 'watcher' and 'watched'. Even the restraint of thoughts or discussions, due to the knowledge they may be recorded for eternity, distorts and twists the free-thinking processes, which are taken for granted.[268]

Australia's involvement in the widespread collection of data on ordinary citizens, reads like a science fiction novel. No longer can the possibility of constant surveillance be relegated to fantasy and the thoughts of the paranoid deluded[269] — systematic surveillance and 'Big Brother' *are here now*. Furthermore, it is paramount to recognise total surveillance is illegitimate[270] — that, just as Kirby J commented, this sort of erosion of fundamental rights grant 'terrorists' success beyond what their own actions could ever achieve.[271]

---

[266] Ibid ch 1 (emphasis added).
[267] Tom Whitehead, 'Email Monitoring: New Powers to Record Every Phone Call and Email Echoes China' *The Telegraph* (online), 1 April 2012 <http://www.telegraph.co.uk/technology/news/9180191/New-powers-to-record-every-phone-call-and-email-makes-surveillance-60m-times-worse.html>.
[268] Richards, above n 258, 1952–61; Bendall and Forte, above n 155, 16; *Draft Resolution — The Right To Privacy In The Digital Age*, 3rd comm, 68th sess, agenda item 69(b), UN Doc A/C.3/68/L.45/Rev.1 (20 November 2013).
[269] See, eg, Renne Grinnell, 'Paranoid Delusion', *PsycCentral* <http://psychcentral.com/encyclopedia/2008/paranoid-delusion/>; Associates in Counselling and Child Guidance, *Delusional Paranoid Disorder*, <http://accg.net/delusional_paranoid_disorder.htm>.
[270] Richards, above n 258, 1961.
[271] *Thomas v Mowbray* (2007) 233 CLR 307 (Kirby J).

IX THE REMEDY

A Bill[272] has been proposed by the Greens, requiring a warrant from the Attorney-General before accessing metadata under the *TIAA*. However, the current legislation has not been able to prevent blanket metadata collection, so even more legislation is unlikely to assist.

Royal Commissions into AIC have been numerous[273] — however, the findings are secret, meaning that any 'sunlight'[274] is quickly darkened.

However, there is one remedy which has evolved in the common law[275] to deal with abuses of the rule of law — judicial review.[276] On point is *Church of Scientology v Woodward*,[277] where ASIO gathered intelligence on parishioners, characterising them to others as security risks. The appellants brought an unsuccessful action for injunctive and declaratory relief. However, the decision clears the way for the High Court to be able to review matters of security and intelligence,[278] and reaffirms High Court jurisdiction.[279] Murphy J considered matters of proof, and due to the secrecy of evidence said the Court must look for 'reasonable grounds that ASIO has misused its powers'.[280]

---

[272] Telecommunications Amendment (Get a Warrant) Bill 2013 (Cth), Senator Scott Ludlam.
[273] See, eg, Commonwealth, Royal Commission on Intelligence and Security *Fourth Report, Volume 1* (1977).
[274] Brandeis J, 'What Publicity Can Do', *Harper's Weekly*, 20 December 1913 <http://www.law.louisville.edu/library/collections/brandeis/node/196> — 'Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.'
[275] Rosanna Panetta, 'Damages for Wrongful Administrative Decisions' (1999) 6 *Australian Journal of Administrative Law* 163, 163.
[276] Standing has been the greatest challenge in the United States of America with the ACLU and Amnesty both being denied standing in *American Civil Liberties Union v Clapper*, (D NY 13 Civ 3994-WHP 12 December 2013); *Clapper v Amnesty International USA*, 568 US 133, 1147 (2013).
[277] (1982) 154 CLR 25.
[278] *Church of Scientology v Woodward* (1982) 154 CLR 25, 59–61 (Mason J), 68 (Murphy J); Nathan Hancock, *Intelligence Services Bill 2001*, No 11 of 2001–02, 1 August 2001, 10-1.
[279] Ibid 65 (Murphy J); *Australian Constitution* s 75(iii) gives the High Court original jurisdiction and s 75(v) allows the Court to issue the writs of mandamus, prohibition and injunction.
[280] Ibid 68 (Murphy J).

Standing could be satisfied under the normal test of special interest,[281] which may require the case to be brought by a body such as Civil Liberties Australia or a relevant law society or legal practice, due to the special interest in maintaining their obligations to clients. It is clear the *Constitution* and rule of law embodied in the common law, *necessitate* the right for judicial review by the High Court.[282] In *A v Hayden*,[283] it was confirmed that the executive must act in 'accordance with the Constitution and the laws of the Commonwealth'.[284]

Judicial review appears to be the only avenue which may hold the executive to account — legislation alone cannot remedy lawlessness.

However, who will have the courage to bring such an action? Who will devote the time and expertise to such a case? Indeed, there are no better experts to understand and advise on such issues than the legal profession. It is the legal profession's role to protect democracy, to act 'in promoting the cause of justice' and 'seek to uphold human rights and fundamental freedoms recognised by national and international law'.[285] It is the profession's duty to push the scales of privacy versus national security back to a level of sanity, fairness and equilibrium. Kirby J commented following the 11 September 2001 bombing of the World Trade Centre:

> We have not done enough for law reform … We have not cared enough for justice. We have just been too busy to repair the holes that we saw. Yet at critical moments in a nation's history, lawyers have upheld the best values of a pluralist democracy. In the future we must do so more wholeheartedly. To preserve liberty we must preserve the rule of law. The rule of law is the

---

[281] *Australian Conservation Foundation v Commonwealth* (1980) 146 CLR 493.
[282] See, eg, *Plaintiff S157/2002 v Commonwealth* (2003) 211 CLR 476; *Enfield City v Development Assessment Commission* (2000) 199 CLR 135; *Australian Communist Party v Commonwealth* (1951) 83 CLR 1; see also Dicey, above n 231, 192-3.
[283] (1984) 156 CLR 532, 595 (Deane J).
[284] Hancock, above n 278, 9.
[285] *Basic Principles on the Role of Lawyers* adopted by the 8th United Nations Congress on the Prevention Of Crime and The Treatment Of Offenders, Havana, Cuba, 27 August, 7 September 1990, A/Conf.144/28/Rev.1, [16], [17], [23].

alternative model to the rule of terror, the rule of money and the rule of brute power. That is our justification as a profession.[286]

[286] Michael, Kirby, 'Australian Law — After 11 September 2001' (2001) 21 Australian Bar Review 253, 264.

X CONCLUSION

The Snowden documents have allowed a glimpse into the secret world of AIC. A glimpse which demonstrates widespread metadata collection, sharing and dissemination and, in some cases, content collection. Metadata is important and at *least* as important as content.

It is clear that retained metadata is immensely valuable to AIC and law enforcement agencies — at any time, the history of an individual can be searched and exposed. Conversely, society has an expectation of privacy in the content of communications, metadata and location data. Jurisprudence, legislation and legal principle supports such expectations. Yet privacy is being invaded on an unprecedented scale, without legislative provision to do so.

The common law, the Magna Carta, the abolition of slavery, and the US and Australian Constitutions, all demonstrate the constant aspiration of freedom. To have come so far in the liberty of man, only to have the interest of national security erode such liberties away, is too disheartening to bear.

Instead, privacy must stand up to take on a fundamental role in the protection of democracy, free society and become again a primary human right. The 'right to be let alone' and to be free from arbitrary surveillance, requires attentiveness, otherwise privacy and liberty are all but dead and buried.

It is time, again, for the legal profession to evoke its place in common law society[287] and stand up for the rights of citizens against the tyranny of the executive.[288] It is all too true that the 'price of freedom *is* eternal vigilance'.

---

[287] Cases such as *Mabo v Queensland (No 2*) (1992) 175 CLR 1, *Plaintiff S157/2002 v Commonwealth* (2003) 211 CLR 476, etc have had the effect of curtailing executive power; the profession have been active against legislation which has removed or limited civil and human rights such as *Anti-Terrorism Act (No 2) 2005* (Cth) which had implications for Dr Mohamed Haneef.

[288] See, eg, Adam J White, 'Tocqueville's "Most Powerful Barrier": Lawyers in Civic Society' (2013) 13 *AEI American Citizenship* <http://www.citizenship-aei.org/2013/09/tocquevilles-most-powerful-barrier-lawyers-in-civic-society/#.UxRP9YW2V5c>; Alexis De Tocqueville, *Democracy in America* as quoted in Diarmuid F O'Scannlain,

EVERYBODY KNOWS

‘The Nobility of the American Lawyer’ (Speech delivered at Commencement Address to the Class of 2013 Chapman University School of Law Chapman University School of Law California 17 May 2013) — ‘When one visits Americans and when one studies their laws, one sees that the authority they have given to lawyers and the influence that they have allowed them to have in the government form the most powerful barrier today against the lapses of democracy.’

BIBLIOGRAPHY

A Articles/Books

Arcila, Fabio JR, 'Dead Ends: *United States v Jones* and the Katz Conundrum' (2012) 9 *North Carolina Law Review* 1

Arcioni, Elisia, 'Developments in Free Speech Law in Australia: Coleman and Mulholland' (2005) 33 *Federal Law Review* 333

Arnold, CA, 'The Reconstitution of Property: Property as a Web of Interests' (2002) 26 *Harvard Environmental Law Review* 281

Bailey, Peter, 'Australia How Are You Going Mate Without a Bill Of Rights? Or Writing the Constitution' (1993) 5 *Canterbury Law Review* 251

Bailey, Peter, *The Human Rights Enterprise in Australia and Internationally* (LexisNexis 2009)

Banisar, D, and Simon Davies, Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments*, <http://gilc.org/privacy/survey/intro.html>

Banks, William C, 'Programmatic Surveillance and FISA: Of Needles in Haystacks' (2010) 88 *Texas Law Review* 1633

Barbas, Samantha, 'Saving Privacy from History' (2012) 61 *Depaul Law Review* 973

Bendall, Anthony and Jason Forte, 'The Privacy Impacts of the Proposed Changes to Australia's National Security Regime' (2012) 9(2) *Privacy Law Bulletin* 14

Bender, David, 'What You Need To Know About NSA Mass Acquisition of Telephony Metadata' (2013) 30 (9) *Computer & Internet Lawyer* 1

Bentham, Jeremy, 'Panopticon of Bentham' in Basil Montagu (ed), *Three Opinions of Different Authors of upon the Punishment of Death* (1813)

Blackshield, Tony and George Williams, *Australian Constitutional Law and Theory Commentary and Materials* (Federation Press, 5th ed, 2010)

Blasberg, Stacy, 'Legal Update Law and Technology of Security Measures in the Wake of Terrorism' (2002) 8 *Boston University Journal of Science and Technology Law* 721

Brandeis, Louis, 'What Publicity Can Do' *Harper's Weekly*, 20 December 1913 <http://www.law.louisville.edu/library/collections/brandeis/node/196>

Brendan, Gerard, 'Australia and the Rule of Law' (2003) *Australian International Law Journal* 1

Breyer, Patrick, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11(3) *European Law Journal* 365

Bronitt, Simon, and Bernadette McSherry, *Principles of Criminal Law* (Lawbook, 3rd ed, 2010)

Bronitt, Simon, and George Williams, 'Political Freedom as an Outlaw: Republican Theory and Political Protest' (1996) 18 *Adelaide Law Review* 289

Bronitt, Simon, and James Stellios, 'Sedition, Security and Human Rights: Unbalanced' Law Reform in the War on Terror' (2006) 30 *Melbourne University Law Review* 923

Butler, Susan (ed), *Macquarie Concise Dictionary* (Macquarie, 5th edition, 2010)

Butt, Peter and David Hamer (eds), *Concise Australian Legal Dictionary* (LexisNexis, 4th ed, 2011)

Cairns, Bernard, *Australia Civil Procedure* (Lawbook, 9th ed, 2011)

Carroll, Elizabeth, '*Woolworths Ltd v Pallas Newco Pty Ltd*: A Case Study in the Application of the Rule of Law in Australia' (2006) 87 *Australian Admin Law Journal* 87

Chemerinsky, Erwin, 'Rediscovering Brandeis's Says Right to Privacy' (2006) 45 *Brandeis Law Journal* 643

Citron Keates, Danielle, and David Gray, 'Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards' (2003) 126 *Harvard Law Review Forum* 262

Cohen, Julie E, 'What Privacy Is For?' (2013) 126 *Harvard Law Review* 1904

Conrad, Sherri, 'Executive Order 12,333: "Unleashing" The CIA Violates the Leash Law' (1985) 70 *Cornell Law Review* 968

Crump, Catherine, 'Data Retention: Privacy, and Anonymity, and Accountability Online' (2013) 56 *Stanford Law Review* 191

Dal Pont, G E, *Lawyers Professional Responsibility* (Lawbook, 5th ed, 2013)

Davis Powel, Connie, 'You Already Have Zero Privacy. Get Over It! Would Warren And Brandeis Argue For Privacy For Social Networking?' (2011) 31 *Pace Law Review* 146

Davis, Martha F, 'Human Rights and Modern Rules of Professional Conduct: Intersection and Integration' (2010) 42 *Columbia Human Rights Law Review* 157

De Tocqueville, Alexis, *Democracy in America* as quoted in O'Scannlain, Diarmuid, 'The Nobility of the American Lawyer' (Speech delivered at Commencement Address to the Class of 2013 Chapman University School of Law Chapman University School of Law California 17 May 2013)

Dicey, AV, *Introduction to the Study of the Law of the Constitution* (Macmillan, 6th ed, 1902)

Emas, Kevin and Tamara Pallas, 'United States v Jones: Does Katz Still Have Nine Lives?' (2012) 24 *St Thomas Law Review* 116

Emerton, Patrick, 'Political Freedoms and Entitlements in the Australian Constitution — An Example of Referential Intentions Yielding Unintended Legal Consequences' (2010) 38 *Federal Law Review* 169

Fitzgerald, Brian et al, *Internet and E–commerce Law* (Lawbook 2011)

Gavison, Ruth, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421

Gaynor, Randy, 'The NSA's Interception of Emails and Phone Calls in the Us Is Unlawful' (2006) 9(8) *Journal of Internet Law* 1

Gerety, Thomas, 'Doing Without Privacy' (1981) 42 *Ohio State Law Journal* 143

Gerety, Tom, 'Redefining Privacy' (1977) 12(2) *Harvard Civil Rights – Civil Liberties Law Review* 233

Ghoshray, Saby, 'Domestic Surveillance via Drones: Looking Through the Lenses of the Fourth Amendment' (2013) 33 *Illinois University Law Review* 579

Goldsworthy, Geoffrey, 'Constitutional Implications Revisited' (2011) 30(1) *University Of Queensland Law Journal* 9

Graves, Lisa, 'The Right to Privacy In Light Of Presidents Programs: What Project Minaret's Admissions Reveal about Modern Surveillance of Americans' (2010) 88 *Texas Law Review* 1855

Gray, Anthony, 'The Common Law and the Constitution as Protectors of Rights in Australia' (2010) 39 *Common Law World Review* 119

Gray, David and Danielle Citron, 'The Right to Quantitative Privacy' (2013) 98 *Minnesota Law Review* 62

Gray, Kevin, 'Property into Thin Air' (1991) 50(2) *Cambridge Law Journal* 252

Gubins, Tamar R, '*Warshak v United States*: The Katz for Electronic Communication' (2008) 23 *Berkeley Technology Law Journal* 723

Heath, William M, 'Possum Processing, Picture Pilfering, Publication and Privacy: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*' (2002) 28 *Monash University Law Review* 162

Hepburn, Samantha, *Australian Property Law Cases Materials and Analysis* (LexisNexis Butterworths, 2nd ed, 2012)

Huxley, Aldous, *Brave New World*, read online as an e-book <http://www.huxley.net/bnw/one.html>

Joseph, Sarah and Melissa Castan, *Federal Constitutional Law, A Contemporary View* (Lawbook, 3rd ed, 2010)

Kelley, Jamuna D, 'A Computer with A View: Progress, Privacy, and Google' (2008) 74 *Brooklyn Law Review* 187

Keyzer, Patrick, *Principles of Australian Constitutional Law* (LexisNexis Butterworths, 3rd ed, 2010)

Kirby, Michael, 'Australian Law — After 11 September 2001' (2001) 21 *Australian Bar Review* 253

Kris, David S, 'On the Bulk Collection of Tangible Things' (2013) 1(4) *Lawfare Research Paper Series* 1

Lauoie, Andrew, 'The Online Zoom Lens: Why Internet Street Level Mapping Technologies Demand Reconsideration of the Modern Day Tort Notion of the "Public"' (2009) 43 *Georgia Law Review* 575

Levy, Leonard, 'Origins of the Fourth Amendment' (1999) 114(1) *Political Science Quarterly* 77

Lim, Cheng and Ike Kutlaca, 'An Explanation of Preservation — Australia's New Data Retention Laws' (2012) *November Internet Law Bulletin* 152

Ludlow, Christina, '"The Gentlest Of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135

McCulloch, Jude and Joo-Cheong Tham, 'Secret State, Transparent Subject: the Australian Security Intelligence Organisation in the Age of Terror' (2005) 38(3) *Australian and New Zealand Journal of Criminology* 400

McGarrity, Nicola and George Williams, 'Counter-Terrorism Laws in a Nation without a Bill of Rights: The Australian Experience' (2010) 2 *City University of Hong Kong Law Review* 45

McGarrity, Nicola, 'An Example of "Worst Practice"? The Coercive Counterterrorism Powers Of the Australian Security Intelligence Organisation' (2010) 4(3) *Vienna Online Journal on International Constitutional Law* 467

McNamara, Jim, and Gail Kenning, 'E Electioneering 2010: Trends in Social Media and Use in Australian Political Communication' (2011) 139 *Media International Australia* 7

McRobert, Andrew, 'Breach of Confidence: Revisiting the Protection of Surreptitiously Obtained Information' (2002) 13 *Australian Intellectual Property Journal* 69

Merrill, TW, 'Property and the Right to Exclude' (1998) 77 *Nebraska Law Review* 730

Meyerson, Denise, 'Why Courts Should Not Balance Rights against the Public Interest' (2007) 31 *Melbourne University Law Review* 873

Michaelsen Christopher, 'International Human Rights on Trial — The United Kingdom's and Australia's Legal Response to 9/11' (2003) 25 *Sydney Law Review* 275

Orwell, George, *1984*, read online as an e-book <http://gutenberg.net.au/ebooks01/0100021.txt>

Panetta, Rosanna, 'Damages for Wrongful Administrative Decisions' (1999) 6 *Australian Journal of Administrative Law* 163

Peikoff, Amy, 'Beyond Reductionism: Reconsidering the Right to Privacy' (2008) 3(1) *New York University Journal of Law & Liberty* 1

Prosser, William, 'Privacy' (1960) 48(3) *California Law Review* 383

Richards, Neil M, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934

Rizk, Hakeem, 'Fundamental Right to Liberty? Online Privacy's Theory for Coexistence with Social Media' (2013) 56 *Howard Law Journal* 951

Robert, McClelland, 'The Future of Security' (2007) 3(4) *Original Law Review* 107

Rodrick, Sharon, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes' (2009) 37 *Federal Law Review* 375

Sauter, Theresa, and Axel Burns, ARC Centre of Excellence for Creative Industries and Innovation, *Social Media in The Media: How Australian Media Perceive Social Media As Political Tools* (2013)

Stephens, Otis, and Richard Glenn, *Unreasonable Searches and Seizures — Rights and Liberties under the Law* (ABC Cilo, 2006)

Taylor, Greg, 'Why Is There No Common Law Right of Privacy?' (2000) 26(2) *Monash University Law Review* 235

Wacks, Raymond, *Understanding Jurisprudence* (Oxford University Press, 3rd ed, 2012)

Walker, Kirsten, 'International Law as a Tool of Constitutional Interpretation' (2001) 28(2) *Monash University Law Review* 86

Walker, Robert, 'Developing The Common Law: How Far Is Too Far?' (2013) 37 *Melbourne University Law Review* 232

Warren, Samuel D, and Louis D Brandeis, 'The Right to Privacy' (1890) 5(IV) *Harvard Law Review* 193

White, Adam J, 'Tocqueville's "Most Powerful Barrier": Lawyers in Civic Society' (2013) 13 *AEI American Citizenship* <http://www.citizenship-aei.org/2013/09/tocquevilles-most-powerful-barrier-lawyers-in-civic-society/#.UxRP9YW2V5c>

Withnall, Sarah, and Michelle Evans, *Administrative Law* (LexisNexis, 2010)

Woessner, Matthew, and Barbara Sims, 'Technological Innovation and the Application of the Fourth Amendment: Considering the Implications of *Kyllo v United States* for Law Enforcement and Counterterrorism' (2003) *Journal of Contemporary Criminal Justice*

B Cases

American Civil Liberties Union v Clapper, (D NY 13 Civ 3994-WHP 12 December 2013)

American Civil Liberties Union v Clapper, (D NY No 13 Civ 3994, 11 June, 2013)

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199

Australian Capital Television Proprietary Ltd v Commonwealth (1992) 177 CLR 106

Australian Communist Party v Commonwealth (1951) 83 CLR 1

Australian Conservation Foundation v Commonwealth (1980) 146 CLR 493

Church of Scientology v Woodward (1982) 154 CLR 25

Clapper v Amnesty International USA, 568 US 133, 1147 (2013)

Coleman v Power (2004) 220 CLR 1

Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission (2002) 313 CLR 543

Doe v Australian Broadcasting Corporation [2007] VCC 281

Enfield City v Development Assessment Commission (2000) 199 CLR 135

Entick v Carrington (1765) 95 ER 807

Griswold v Connecticut, 381 US 479 (1965)

Grosse v Purvis (2003) QDC 151

Katz v United States, 389 US 347 (1967)

Khorasandjian v Bush (1993) QB 727

Klayman v Obama, (D DC, Dkt # 13 (No 13-0851), # 10 (No 13-0881, 16 February 2013) Memorandum Opinion 58

Kyllo v United States, 190 F 3d 1041 (9th Cir, 1999)

Lange v Australian Broadcasting Corporation (1997) 189 CLR 520

Mabo v Queensland (No 2) (1992) 175 CLR 1

Marbury v Maddison, 5 US 137, 177 (1803)

Nationwide News Pty Ltd v Wills (1992) 177 CLR 1

Olmstead v United States, 277 US 438, (1928)

Pavesich v New England Life Insurance Co, 50 SD 68 (1905)

People v Weaver, 12 NY 3d 433 (2009)

Plaintiff S157/2002 v Commonwealth (2003) 211 CLR 476

Prince Albert v Strange (1849) 49 ER 1302

R v Giannakopoulos [2013] SASCFC 50

Roberson v Rochester Folding Box Company, 64 NY 422 (1902)

Roe v Wade, 410 US 113 (1973)

Smith v Jones [1999]1 SCR 455

Smith v Maryland, 422 US 735 (1979)

Thomas v Mowbray (2007) 233 CLR 307

United States v Jones, 132 US 945 (2012)

United States v Knotts, 460 US 276 (1983)

United States v Kyllo, 1996 US 3864 (15 March 1996) Affidavit, 190 F 3d 1041 (9th Cir 1999) Reviewed 533 US 27 (2001)

United States v Kyllo, 533 US 27 (2001)

United States v Maynard, 615 F 3d 568 (2010)

Vacated *Warshak v United States,* No 06-4092, 2007 US App LEXIS 23741 (6th Cir 9 October 2007)

Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479

Warshak v United States, (No 1:06-cv-357, 2006) US Dist LEXIS 50076, (SD Ohio 2007)

Warshak v United States, 490 F 3d 455 (6th Cir, 2007)

Warshak v United States, No 06-4092, 2007 US App LEXIS 23741 (6th Cir 9 October 2007)

Whitney v California, 274 US 357 (1927)

Wilkes v Wood (1763) 19 Howell's State Trials 1153

Wyatt v Wilson (1820) unreported

C Legislation

American Law Institute, Restatement (Second) of Torts (1976) SEC 652C

Anti-Terrorism Act (No 2) 2005 (Cth)

Australian Constitution

Australian Constitution.

Australian Secret Intelligence Service, Australian Government, *Privacy Rules* <http://www.asis.gov.au/Privacy-rules.html>

Australian Security Intelligence Organisation Act 1979 (Cth)

Australian Security Intelligence Organisation Act 1979 (Cth)

Defence Signals Directorate, Australian Government, *Privacy Rules, Rules to Protect the Privacy of Australians,* <http://www.asd.gov.au/publications/dsdbroadcast/20121002-privacy-rules.htm>

Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth)

Inspector General of Intelligence and Security Act 1986 (Cth)

Intelligence Services Act 2001 (Cth)

Privacy Act 1988 (Cth)

Stored Communications Act 18 USC § 2703(a) (2000 & Supp 2005)

Surveillance Devices Act 1998 (WA)

Surveillance Devices Act 2004 (Cth)

Telecommunications (Interception and Access) Act 1979 (Cth)

Telecommunications Act 1997 (Cth)

Telecommunications Amendment (Get a Warrant) Bill 2013 (Cth)

United States Constitution

Workplace Surveillance Act 2005 (NSW)

D UN Documents/Declarations

Basic Principles on the Role of Lawyers adopted by the 8th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August, 7 September 1990, A/Conf.144/28/Rev.1

CCPR General Comment Number 16: Article 17 (Right To Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour And Reputation, 3rd Comm, 32nd Sess (8 April 1988)

Draft Resolution — The Right to Privacy in the Digital Age, 3rd comm, 68th sess, agenda item 69(b), UN Doc A/C.3/68/L.45/Rev.1 (20 November 2013)

International Covenant On Civil And Political Rights International Covenant on Civil and Political Rights, opened for signature 16 December 1966, ratified Australia 13 November 1980, 999 UNTS 171 (entered into force 23 March 1976)

Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948)

E Reports/Inquiries/Royal Commissions/Bill Digests

Attorney-General's Department, Australian Government, *Telecommunications (Interception and Access) Act 1979, Annual Report 2012-13*

Australian Communications and Media Authority, *Communications Report 2011–12 Series, Report 3—Smartphones and tablets Take-up and use in Australia* (2013)

Australian Communications and Media Authority, *Communications Report 2011–12 Series, Report 2—Australia's Progress in the Digital Economy, Participation, Trust and Confidence* (2012)

Australian Law Reform Commission, *For Your Information: Australian Privacy and Law Practice*, Report No 108 (2008)

Cavoukian, Ann, Information and Privacy Commissioner, Ontario Canada, *A Primer on Metadata: Separating Fact from Fiction'* July 2013 <http://www.privacybydesign.ca/index.php/paper/a-primer-on-metadata-separating-fact-from-fiction/>

Commonwealth, Royal Commission on Intelligence and Security *Fourth Report, Volume 1* (1977)

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the US NSA Surveillance Program, Surveillance Bodies in Various Member States and the Impact on EU Citizens of Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*, Doc No 2013/2188 (INI), 8 January 2014

Ewing, Scott, and Julian Thomas, ARC Centre of Excellence for Creative Industries and Innovation, *CCi Digital Futures 2010 the Internet in Australia* (2010)

Hancock, Nathan, Information and Research Services, Parliament of Australia, *Intelligence Services Bill 2001*, No. 11 2001-02 of 2001, 1 August 2001

Hancock, Nathan, *Intelligence Services Bill 2001*, No 11 of 2001–02, 1 August 2001

Inspector General of Intelligence and Security, Australian Government, *Annual Report 2012 – 2013*

Inspector General of Intelligence and Security, *Report MV Tampa, August – September 2001 – Collection and Reporting of Intelligence Relating to Australians* Document Number 20502/02 <http://www.defence.gov.au/minister/13tpl.cfm?CurrentId=1441>

Leveson LJ, Leveson Inquiry, *The Report into the Culture, Practices and Ethics of the Press*, 29 November 2012 <http://www.levesoninquiry.org.uk/>

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013

Ubiquitous Computing — International Telecommunications Union, 'The Internet of Things', (2005) <http://www.itu.int/osg/spu/publications/internetofthings/>

F Online Newspapers/Internet Materials/Media Releases/Transcripts

'City of London Corporation Wants "Spy Bins" Ditched', *The Guardian* (online), 13 August 2013 <http://www.theguardian.com/world/2013/aug/12/city-london-corporation-spy-bins>

'Greenwald: "Explosive" NSA Spying Reports Are Imminent', *Spiegel Online International* (online), 19 July 2013 <http://www.spiegel.de/international/world/journalist-says-explosive-reports-coming-from-snowden-data-a-912034.html>

'How the NSA Is Tracking People Right Now', *The Washington Post* (online), <http://apps.washingtonpost.com/g/page/world/how-the-nsa-is-tracking-people-right-now/634/>

'NSA Defends Global Cellphone Tracking', *news.com.au* (online), 7 December 2013 <http://www.news.com.au/world/breaking-news/nsa-defends-global-cellphone-tracking/story-e6frfkui-1226777696658>

'XKeyscore Presentation from 2008 – Read in Full', *The Guardian* (online), 31 July 2013 <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>

AAP, 'US Government Appeals Ruling on NSA Data Program', *SBS* (online), 4 January 2014 <http://www.sbs.com.au/news/article/2014/01/04/us-govt-appeals-ruling-nsa-data-program>

Ackerman, Spencer, 'NSA Statement Does Not Deny Spying on Members Of Congress', *The Guardian* (online), 5 January 2014 <http://www.theguardian.com/world/2014/jan/03/nsa-asked-spying-congress-bernie-sanders>

Ackerman, Spencer, and Dan Roberts, 'The Obama Presents NSA Reforms with Planned to End Government Storage of Call Data', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/world/2014/jan/17/obama-nsa-reforms-end-storage-americans-call-data>

Ackerman, Spencer, and Dominic Rushe, 'Microsoft, Facebook, Google and Yahoo Release US Surveillance Requests', *The Guardian* (online), 4 February 2014 <http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests>

Allard, Tom, 'Intelligence Agency Failed To Investigate Spying Claims, Lawyer Bernard Collaery Claims', *Sydney Morning Herald* (online), 5 December 2013 <http://www.smh.com.au/federal-politics/political-news/intelligence-agency-failed-to-investigate-spying-claims-lawyer-bernard-collaery-claims-20131204-2yr3m.html>

American Civil Liberties Union <https://www.aclu.org/>

Associates in Counselling and Child Guidance, *Delusional Paranoid Disorder*, <http://accg.net/delusional_paranoid_disorder.htm>

Australia Federation Press, 'US "Spied On Radicals" Porn Habit, According To Documents from Edward Snowden', *The Australian* (online), 28 November 2013 <http://www.theaustralian.com.au/news/world/us-spied-on-radicals-porn-habits-according-to-documents-from-edward-snowden/story-e6frg6so-1226770374222>

Australian Associated Press, 'Government Defends ASIO Raids', *Perth Now* (online), 4 December 2013 <http://www.perthnow.com.au/news/breaking-news/brandis-defends-asio-spy-raids/story-fnhrvfuw-1226775148265>

Australian Broadcasting Corporation, 'In Google We Trust', *Four Corners*, 10 September 2013 <http://www.abc.net.au/4corners/stories/2013/09/09/3842009.htm>

Ball, James, 'How Obama Took on Six Major Areas of Concern about NSA Surveillance', *The Guardian*, (online), 18 January 2014 <http://www.theguardian.com/world/2014/jan/17/how-obama-took-on-six-major-areas-concern-nsa-surveillance>

Ball, James, 'NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show', *The Guardian* (online), 1 October 2013 <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>

Brennan, Frank, 'ASIO Raids Designed to Show Timor Who's Boss', *The Age* (online), 5 December 2013 <http://www.theage.com.au/comment/asio-raids-designed-to-show-timor-whos-boss-20131204-2yqxq.html>

Buckley, Nick, 'More Spy Leaks to Come: Minister', *The West Australian* (online), 3 December 2013 <http://au.news.yahoo.com/thewest/latest/a/20119934/more-spy-leaks-to-come-minister/>

Chadwick, Paul, 'Balancing Security and Privacy: Bob Hawke Faced Dilemmas Familiar Today', *The Guardian* (online), 1 January 2014 <http://www.theguardian.com/world/2013/dec/31/balancing-security-and-privacy-bob-hawke-faced-dilemmas-familiar-today>

Civil Liberties Australia <http://www.cla.asn.au/>

Crook, Clive, 'Is The US Still The Land Of The Free?', *Bloomberg* (online), 11 June 2013 <http://www.bloomberg.com/news/2013-06-11/is-the-u-s-still-the-land-of-the-free-.html>

Curnyn, Sean, 'Everybody Knows (Starting with the NSA)', *The Cinch Review* (online), 13 June 2013 <http://www.cinchreview.com/everybody-knows-starting-with-nsa/10482/>

Davies, Trefor, 'Government Web Surveillance: "Expensive, Impractical, Totalitarianism"', *The Telegraph* (online), 02 April 2012 <http://www.telegraph.co.uk/technology/news/9180577/Government-web-surveillance-Expensive-impractical-totalitarian.html>

Dorling, Phillip, 'Australian Spies in Global Deal to Undersea Cables', *Sydney Morning Herald* (online), 29 August 2013 <http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html>

Dworkin, Ronald, 'A Special Supplement: Taking Rights Seriously', (1970) *The New York Review of Books* <http://www.nybooks.com/articles/archives/1970/dec/17/a-special-supplement-taking-rights-seriously/>

Farrell, Paul, 'History of Five Eyes — Explainer', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>

Farrell, Paul, 'Intelligence Agencies Should Be Subject To FoI, Haitian, Says Information Commissioner', *The Guardian* (online), 4 February 2014 <http://www.theguardian.com/world/2014/feb/03/intelligence-agencies-foi-laws>

Gabbatt, Adam, 'Obama Acknowledges Edward Snowden Disclosures in NSA Reform Speech', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/world/2014/jan/17/obama-acknowledges-edward-snowden-nsa-reform>

Gaouette, Nicole, 'Microsoft, Google Security: Edward Snowden Won Where Barack Obama Failed', *Live Mint* (online), 29 November 2013 <http://www.livemint.com/Consumer/ZD6Bc7SRBoOib9bLbsRSPN/Microsoft-Google-security-Edward-Snowden-won-where-Barack.html>

Gellman, Barton and Soltani, Ashkan, 'NSA Infiltrates Links to Yahoo, Google Data Centres Worldwide, Snowden Documents Say', *The Washington Post* (online), <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>

Gellman, Barton, 'Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished,' *The Guardian* (online), 24 December 2013 <http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html>

Gellman, Barton, and Ashkan Soltani, 'NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show', *The Washington Post* (online), 5 December 2013 <http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html>

Golgowski, Nina, 'How Target Knows When Its Shoppers Are Pregnant – and Figured out a Teen Was before Her Father Did', *The Daily Mail* (online), <http://www.dailymail.co.uk/news/article-2102859/How-Target-knows-shoppers-pregnant--figured-teen-father-did.html#ixzz2uOkwgc3X>

Greenwald, Glenn 'NSA Prism Program Taps In To User Date Of Apple, Google And Others', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

Greenwald, Glenn, 'Obama's NSA "Reforms" Are Little More Than a PR Attempt to Mollify the Public', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/commentisfree/2014/jan/17/obama-nsa-reforms-bulk-surveillance-remains>

Greenwald, Glenn, and Ewen McAskill, 'NSA Prism Program Taps In To User Data Of Apple, Google And Others', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

Greenwald, Glenn, Ewen MacAskill and Laura Poitras, 'Edward Snowden: The Whistle-Blower behind the NSA Surveillance Revelations', *The Guardian* (online), 10 June 2013 <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

Greenwald, Glenn, Ewen MacAskill and Laura Poitras, 'Edward Snowden: The Whistle-blower behind the NSA Surveillance Revelations', *The Guardian* (online), 10 June 2013

<http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

Greenwald, Glenn, Gallagher, Ryan and Grim, Ryan, 'Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit "Radicalizers"', *The Huffington Post* (online), 26 November 2013< http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html>

Grinnell, Renne, 'Paranoid Delusion', *PsycCentral* <http://psychcentral.com/encyclopedia/2008/paranoid-delusion/>

Hodson, Hal, 'How Metadata Brought Down CIA Boss David Petrous', *The New Scientists* (online), 16 November 2012 <http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html#.UxDQZoW2V5d>

Hopkins, Nick, 'Huge Swathes of GCHQ Mass Surveillance Is Illegal, Says Top Lawyer', *The Guardian* (online), 29 January 2014 <http://www.theguardian.com/uk-news/2014/jan/28/gchq-mass-surveillance-spying-law-lawyer>

Hopkins, Nick, and Ian Traynor, 'NSA and GCHQ Activities Appear Illegal, Says EU Parliamentary Enquiry', *The Guardian* (online), 10 January 2014 <http://www.theguardian.com/world/2014/jan/09/nsa-gchq-illegal-european-parliamentary-inquiry>

Horgan, John, 'US Never Really Ended Creepy "Total Information Awareness" Programme', *Scientific American* (online), 7 June 2013 <http://blogs.scientificamerican.com/cross-check/2013/06/07/u-s-never-really-ended-creepy-total-information-awareness-program/>

Hunter, Melanie, 'Deputy AG: Governments Meta Data Collection May Have Resulted in One Criminal Case', *CNS News* (online), 4 February 2014 <http://cnsnews.com/news/article/melanie-hunter/deputy-ag-government-s-metadata-collection-may-have-resulted-one>

Isquith, Elias, 'Reports: NSA Spied on Online Sexual Habits of Muslims to Discredit "Radicalisers"', *Salon* (online), 27 November 2013 <http://www.salon.com/2013/11/27/report_nsa_spied_on_online_sexual_habits_of_muslims_to_discredit_radicalizers/>

Jabour, Birdie, 'Australia Spied on Indonesia Talks with US Law Firm In 2013', *The Guardian* (online), 16 February 2014 <http://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm>

Kay, Jonathan, 'We All Have Something to Hide From Big Brother, We Just Don't Know It Yet', *National Post* (online), 14 June 2013 <http://fullcomment.nationalpost.com/2013/06/14/we-all-have-something-to-hide-from-big-brother-we-just-dont-know-it-yet/>

Keane, Bernard, 'Australia's Supine Reaction to our Surveillance Planet', *Crikey* (online), 14 June 2013 <http://www.crikey.com.au/2013/06/14/australias-supine-reaction-to-our-surveillance-planet/>

Kelley, Michael, 'NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them', *Business Insider Australia* (online), 14 December 2013 <http://www.businessinsider.com.au/how-many-docs-did-snowden-take-2013-12>

Kravets, David, 'Reading between the Lines of Redacted NSA Documents', *Wired* (online), 19 February 2014 <http://www.wired.com/threatlevel/2014/02/nsa-gallery/>

Laughland, Oliver, 'Metadata: Is It Simply "Billing Data", or Something More Personal?', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/metadata-should-it-be-dismissed-as-billing-data-or-is-it-personal-material>

Lemay, Renai, 'Labour Open to Surveillance Discussion', *Delimiter* (online), 4 December 2013 <http://delimiter.com.au/2013/12/04/labor-open-surveillance-discussion/>

Lennard, Natasha, 'Secret Deal let NSA Spy on Ordinary UK Citizens', *Salon* (online), 21 November, 2013 <http://www.salon.com/2013/11/21/secret_deal_let_nsa_spy_on_ordinary_u_k_citizens/>

Lennard, Natasha, 'UN to Investigate NSA, GHCQ Spying', *Salon* (online), 3 December 2013 <http://www.salon.com/2013/12/03/u_n_to_investigate_nsa_ghcq_spying/>

Lennard, Natasha, and Glenn Greenwald, 'Here Is How to Stop the NSA', *Salon* (online), 1 October 2013 <http://www.salon.com/2013/10/01/greenwald_surveillance_power/>

Leonard, Andrew, Dave Eggers, 'To The Internet: Just Stop!', *Salon* (online), 8 October 2013 <http://www.salon.com/2013/10/08/dave_eggers_to_the_internet_just_stop/>

Leonhard, Andrew, 'Turnkey Totalitarianism', *Salon* (online), 17 June 2013 <http://www.salon.com/2013/06/17/turnkey_totalitarianism/>

Lewis, Paul, 'Snowden Documents Show NSA Gathering 5,000,000,000 Cell Phone Records Daily', *The Guardian* (online), 5 December 2013 <http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden>

Linklater, Alexander, 'The Circle, by Dave Eggers — Book Review', *The Guardian* (online), 13 October 2013 <http://www.theguardian.com/books/2013/oct/12/the-circle-dave-eggers-review>

McAskill, Ewen, 'NSA Collected Details Of Online Sexual Activity of Islamist Radicals', *The Guardian* (online), 27 November 2013 <http://www.theguardian.com/world/2013/nov/27/nsa-details-online-sexual-activity-islamist-radicals>

McAskill, Ewen, James Ball and Katherine Murphy, 'Revealed: Australian Spy Agency Offered to Share Data about Ordinary Citizens', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>

McCarthy, Tom, 'Obama Announces New Limits on NSA Surveillance Programs Live Reaction', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/world/2014/jan/17/obama-nsa-surveillance-reforms-speech-live>

Mcstravick, Alan, 'UK Intelligence Using NSA Technique to Spy on Citizens: Snowden', *Red Orbit* (online), 12 November 2013 <http://www.redorbit.com/news/technology/1113000232/edward-snowden-claims-uk-spying-nsa-techniques-111213/>

Mezrani, Leanne, 'Spying Case Raises Questions Of Liability', *Lawyers Weekly* (online), 25 February 2014 <http://www.lawyersweekly.com.au/news/spying-case-raises-concerns-about-law-firm-liabili?utm_source=Cirrus+Media+Newsletters&utm_campaign=21b70018d3-Lawyers+Weekly+Newsletter+-+20140225111724&utm_medium=email&utm_term=0_fe913f1856-21b70018d3-59556813>

Michaelsen, Chris, 'No Secret, This Spying Stinks', *The Canberra Times* (online), 6 December 2013 <http://www.canberratimes.com.au/comment/no-secret-this-spying-stinks-20131205-2ytm5.html>

Murphy, Katherine, 'Australia's Surveillance Has "Achieved Too Much" to Stop, Says David Johnson', *The Guardian* (online), 3 December 2013 <http://www.theguardian.com/world/2013/dec/03/australias-surveillance-achieved-too-much-to-stop-david-johnston/print>

O'Carroll, Lisa, 'Rebekah Brooks to Begin her Defence at Phone-hacking Trial', *The Guardian* (online), <http://www.theguardian.com/uk-news/2014/feb/18/rebekah-brooks-defence-phone-hacking-trial-andy-coulson?CMP=ema_546>

Ockenden, Will, 'Australia Prepared Briefing On US Global Internet Spying Program Prism Before Snowden Revelations', *ABC News* (online), 8 October 2013 <http://www.abc.net.au/news/2013-10-08/australia-prepared-briefing-on-prism-spying-program/5004290>

Office of the High Commissioner for Human Rights, 'Mass Surveillance: Pillay Urges Respect for Right to Privacy and Protection of Individuals Revealing Human Rights Violations', (Media Release, 2 July 2013) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13534&>

Pengelly, Martin, 'US Law Firm Was Caught in NSA Surveillance Net in Indonesia — Report', *The Guardian* (online), <http://www.theguardian.com/world/2014/feb/15/us-law-firm-nsa-surveillance-indonesia-australia>

Pfaffenbach, Kai, 'Australian Government Talked PRISM Before Snowden Revelations', *RT News* (online), 8 October 2013 <http://rt.com/news/australia-knew-prism-before-879>

Roberts, Dan and Spencer Ackerman, 'Obama Review Panel: Strip NSA of Power to Collect Phone Data Records', *The Guardian* (online), 19 December 2013 <http://www.theguardian.com/world/2013/dec/18/nsa-bulk-collection-phone-date-obama-review-panel>

Robertson, Geoffrey, 'The Privacy of Ordinary Australians Is under Serious Threat', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/commentisfree/2013/dec/02/privacy-australians-surveillance-metadata>

Rowlings, Bill, 'The Public Deserves a Spy Inquiry Now', *New Matilda* (online), 5 December 2013 <https://newmatilda.com/2013/12/05/public-deserves-spy-inquiry-now>

Rushe, Dominic and James Ball, 'Prism Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining>

Rushe, Dominic, 'UN Advances in Surveillance Resolution Reaffirming Human Right to Privacy', *The Guardian* (online), 27 November 2013

<http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy>

Saarinen, Juha, 'Aussie Government Knew Of PRISM And Ahead of Snowden Leaks', *IT News* (online), 8 October 2013 <http://www.itnews.com.au/News/359750aussie-govt-knew-about-prism-ahead-of-snowden-leaks.aspx>

Sanchez, Julian, 'A Reply to Epstein and Pilon on NSA's Metadata Program', *Cato Liberty* (online), 16 June 2013 <http://www.cato.org/blog/reply-epstein-pilon-nsas-metadata-program>

Sanchez, Julian, 'How Rand Paul Can Take on the NSA', *Bloomberg* (online), 11 June 2013 <http://www.bloomberg.com/news/2013-06-11/how-rand-paul-can-take-on-the-nsa.html>

Siddique, Haroon, 'Internet Privacy as Important as Human Rights Says UN's Navi Pillay', The Guardian (online), 27 December 2013 <http://www.theguardian.com/world/2013/dec/26/un-navi-pillay-internet-privacy>

Taylor, Lenore, 'Australians will Be Troubled by Google, Facebook and Our Poor Surveillance by US', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/07/australians-troubled-us-surveillance-google-facebook-apple>

Telecommunications Interception and Access Laws, Electronic Frontiers Australia <https://www.efa.org.au/Issues/Privacy/tia.html>

The Guardian, *The NSA Files* <http://www.theguardian.com/world/the-nsa-files>

Traynor, Ian, Philip Oltermann, and Patrick Wintour, 'Obama NSA Reforms Receive Mixed Response in Europe and Brazil', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/world/2014/jan/17/obama-nsa-reforms-reaction-europe-brazil>

Whitehead, Tom, 'Email Monitoring: New Powers to Record Every Phone Call and Email Echoes China' *The Telegraph* (online), 1 April 2012

<http://www.telegraph.co.uk/technology/news/9180191/New-powers-to-record-every-phone-call-and-email-makes-surveillance-60m-times-worse.html>

Whitehead, Tom, 'Email Monitoring: New Powers to Record Every Phone Call and Email Echoes China', *The Telegraph* (online), 1 April 2012 <http://www.telegraph.co.uk/news/uknews/law-and-order/9179117/Email-monitoring-New-powers-to-record-every-phone-call-and-email-echoes-China.html>

Wilentz, Sean, 'Would You Feel Differently about Snowden, Greenwald and Assange If You Knew What They Really Thought?', *New Republic* (online), 19 January 2014 <http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe>

Wittes, Benjamin, and Hasan Dinjer, 'Takes a Look at the Parliamentary Legal Advice on GCHQ Surveillance', *Lawfare Hard National Security Choices* (online), 2 February 2014 <http://www.lawfareblog.com/2014/02/hasan-dindjer-takes-a-look-at-the-parliamentary-legal-advice-on-gchq-surveillance/#.UwQz_IWPuxk>

Wolf, Naomi, 'The New Totalitarianism of Surveillance Technology', *The Guardian* (online), 16 August 2012 <http://www.theguardian.com/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology>

Womack, Brian, and Sylvia Wier, 'Facebook Releases Information on Security Data Requests', *Bloomberg* (online), 15 June 2013 <http://www.bloomberg.com/news/2013-06-15/facebook-releases-information-on-security-data-requests.html>

EVERYBODY KNOWS

G Other

Leonard Cohen, *Everybody Knows* (I'm Your Man, 1988)

Letter from Martin Brandy, Director, Defence Signals Directorate to Ross Colthart, Reporter, *Sunday Program* 16 March 1999 <http://cryptome.org/jya/dsd-sigint.htm>