Let Me and My Metadata Alone: Australia's Compliance with Article 17 of the International Covenant on Civil and Political Rights

THIS THESIS IS SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF RESEARCH (MRES), COMPLETED AT THE MACQUARIE LAW SCHOOL WITHIN THE FACULTY OF ARTS, MACQUARIE UNIVERSITY, NSW.

PAUL MALUGA, 24 APRIL 2017

I. SUMMARY **2**

II. STATEMENT BY THE AUTHOR **3**

III. ACKNOWLEDGEMENTS **4**

I INTRODUCTION **5**

A *Defining Privacy* 7
B *Characterising 'Privacy' and its Significance* 8

II PRIVACY: THREE WAVES OF DEVELOPMENT **11**

A *First Wave* 11
B *Second Wave* 12
C *Third Wave* 13

III PRIVACY, METADATA RETENTION AND SOLOVE'S TAXONOMY **16**

A *Information Collection* 16
1 Surveillance *16*
B *Information Processing* 18
1 Aggregation *18*
2 Identification *18*
3 Insecurity *19*
4 Secondary Use *19*
C *Information Dissemination* 20
1 Disclosure *20*
D *Invasion* 20
1 Intrusion *20*

IV PRIVACY IN INTERNATIONAL LAW **21**

A *International Bill of Human Rights* 21
1 Universal Declaration of Human Rights *22*
2 International Covenant on Civil and Political Rights *22*
B *Article 17 of the International Covenant on Civil and Political Rights* 23
1 Unlawful and Arbitrary Interference with Privacy *24*
(a) Meaning of 'Unlawful' 24
(b) Meaning of 'Arbitrary' 26
(i) Necessity, Legitimacy and Proportionality 26

V METADATA RETENTION IN AUSTRALIA **27**

A *2008 Law Reform Commission Report* 27
B *2013 PJCIS Report* 28
C *Metadata Retention Legislation* 32
1 Journalist Information Warrant and the Public Interest Advocate *33*
2 Additional Impacts of the TIA Act Amendments *35*
D *Parliamentary Inquiries into the Amendment of the TIA Act* 37
1 International Standard of Privacy Protection *38*
(a) Is Metadata Retention Effective? 39
(b) Is Metadata Retention Necessary? 42
(c) Is Metadata Retention a Proportionate Response to the Outlined Threat? 49

VI CONCLUSION **57**

VII REFERENCES **60**

ANNEXURE A: HISTORY OF PRIVACY PROTECTION IN AUSTRALIA **68**

ANNEXURE B: EXTRACT FROM SECTION 187AA(1) OF THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979* (CTH) **71**

i. Summary

In 2015, Australia enacted legislation to require telecommunications service providers to retain user and subscriber metadata for a period of two years. The retention of metadata, classified under legislation as personal information, raises concerns of the potential of unlawful privacy intrusions into the private lives of individuals by state and non-state actors. The aim of this research is to evaluate whether the legislation is consistent with Australia's obligations under article 17 of the *International Covenant on Civil and Political Rights*. This paper explores the development of the concept of privacy as a human right and illustrates that privacy concerns closely followed with advances in technology, capable of being delineated into three waves of privacy discourse. Daniel Solove's taxonomy of privacy is used to analyse threats to privacy engendered by metadata retention. Using international legal instruments, this research offers a set of requirements that must be satisfied for privacy intrusions to be deemed legitimate, necessary and proportionate. Upon applying the international legal requirements to the metadata retention legislation, this research concludes that Australia does not meet its international legal obligations to protect individual privacy against unlawful or arbitrary interference.

ii. STATEMENT BY THE AUTHOR

This these is submitted in fulfillment of the requirement of the degree of Masters of Research completed at the Macquarie Law School within the Faculty of Arts.

This thesis has not previously been submitted previously for a higher degree at this or any other institution. This thesis represents the author's original work except as acknowledged by way of references.

_____

Signature

24 April 2017

Date

iii. Acknowledgements

The author wishes to thank Carolyn Adams for her invaluable insight, unwavering support, and patience in providing supervision for this dissertation. Additionally, the author wishes to express gratitude to George F. Tomossy and Zara J. Bending for their collegiality and hard work without which a publication arising from sections 3 and 5 of this dissertation would not have been possible (further thanks to the editorial board and reviewers of the Journal of Ethics, Medicine and Public Health for their feedback and constructive criticism). Finally, the author is grateful to the wider Macquarie Law School community and in particular, Dr Shireen Daft, Dr Roy Baker, Dr David Mullan, and Mr Kevin Yee.

I INTRODUCTION

Technological development invariably influences how individuals interact with each other and has the capacity to augment the relationship between the individual and the State, depending on how either party chooses to utilise new technology. For example, technological advancement has demonstrably impacted the notion of what is considered 'private' versus 'public'. The invention of the 'instanenuous photographs' at the turn of the 20th century brought with it a series of questions about what ought to be considered personal information and what citizens could reasonably expect to be the bounds of the 'private domestic life';[1] this discourse would provide some of the earliest debates about the practical meaning of privacy and the extent of legal protection. Indeed, in the modern era (from the late 19th century onwards), privacy debates followed closely with developments in technology including the invention and domestic consumption of computers and internet services. Currently, in the digital age, privacy has become an increasingly contested concept – on the one hand, the value of privacy in a democratic society features prominently in the literature on liberty, equality, and the utility of privacy;[2] on the other, there are legitimate reasons for governments to curtail certain aspects of privacy – for instance, in the interest of public safety. The global reach and ubiquitous use of the internet now mean that threats to a government and its people that were once isolated to specific countries or global regions can now impact the global community – this is becoming clear with the increasing use of encryption by terrorists in their communications.[3] However, in the search for public safety, governments are increasingly resorting to limitations on individual privacy and other rights – for instance, the disclosure by Edward Snowden in 2013 about the global collection of electronic telecommunications information perpetrated by the United States' National Security Agency ('**NSA**') and their partners in the 'Five Eyes': Australia, United Kingdom, Canada, and New Zealand bear this out – particularly as the disclosure made clear that even telecommunication content was being intercepted.[4] These disclosures indicate that the NSA, chiefly, and their intelligence-gathering partners, engaged in mass processing of a majority of all global telecommunications traffic, including against their citizens as well as other innocent civilians globally,

---

[1] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193, 195.

[2] This perspective features prominently in literature, see, eg: James Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113(6) *Yale Law Journal* 1151; David Lindsay, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29(1) *Melbourne University Law Review* 131; William Pitt, *Speech on the Excise Bill*, House of Commons, Parliament of the United Kingdom (March 1763); Peter Swire, 'Financial Privacy and the Theory of High-Tech Government Surveillance' (1999) 77 *Washington University Law Quarterly* 461; John Gilliom, *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy* (Chicago University Press, 2001); Richard Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553.

[3] See, eg, Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (Scribe Publications, 2002) 76.

[4] See, eg, Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded. What the revelations mean for you', *The Guardian (The Australian Edition)* (online), 01 November 2013 <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

and show the lengths that some states are willing to go to gather intelligence for military and policing purposes. The purpose of the present thesis is to focus on a particular, more limited instance of undue government intrusion into the personal information of individuals.

In 2015, the Australian Government enacted legislation requiring all telecommunications service providers to retain their subscribers' metadata for a period of two years.[5] This was said to be a legitimate response to threats to Australia and its population, including serious crime and threats to national security. However, concern has been raised about whether this legislation complies with Australia's international legal obligations, and there emerges a specific question as to its obligations under article 17 of the *International Covenant on Civil and Political Rights* ('**ICCPR**')[6] which requires state parties to ensure protection of individual privacy against unlawful or arbitrary interference. This dissertation examines whether Australia's metadata retention legislation is consistent with its international under article 17 by undertaking a seven-part examination. The research is conducted on a doctrinal basis, examining both primary sources of law in the domestic and international context, together with the writings on the topic by preeminent jurists and academics from circa 1890 to the present moment. It commences with an introduction to the scholarly discourse on privacy, including the omnipresent problem of 'defining privacy'. The second section more exhaustively analyses the concept of privacy, including early efforts at legal protection, and categorises conceptual development into three distinct 'waves of privacy' which emerged as a result of technological innovation. The third section will then delineate the various privacy concerns arising from metadata retention in light of the theoretical underpinnings of privacy within the current Third Wave of academic discourse, using Solove's 'Taxonomy of Privacy Problems'. Solove's Taxonomy was chosen as the theoretical framework to base the doctrinal analysis of legislation due to its broad-based encapsulation of relevant privacy problems. The fourth section subsequently examines the international standard of privacy protection and derives the relevant legal test against which the *Telecommunications (Interception and Access) Act 1979* (Cth) ('**the TIA Act**') will be analysed. In brief, the test is comprised of three prongs, whereby a law must: (i) be necessary to fulfil a legitimate aim; (ii) be effective in achieving that aim; and (iii) not enlist measures that disproportionately burden or intrude on the right to privacy against the aim sought. Finally, the fifth and sixth sections will answer the research question posed by critically analysing Australia's metadata retention laws against the legal test provided in section four. The central claim of this dissertation is that the Australian metadata retention regime is a fundamental and problematic infringement of individual privacy from a theoretical perspective that, in addition, does not meet the legal standard established under

[5] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187C.

[6] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('*ICCPR*').

international law for a permissible intrusion into individual privacy, most notably owing to its disproportionality.

A *Defining Privacy*

The Macquarie Dictionary defines 'privacy' as 'the state of being private; retirement or seclusion; secrecy'.[7] In addition, the Oxford English Dictionary provides that privacy is '[t]he state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion'.[8] While these definitions appear to be comprehensive, the reality is that the concept of privacy and notions of privacy intrusions are highly contested, culturally-determined and subject to evolution due to technological advancement and the prevailing political landscape. Since being put forward as a concrete right by Warren and Brandeis in the late 19th century,[9] privacy has been seen as a principle affecting individual liberty, resulting in the need to find a balance between competing liberty rights.[10] This can be seen, for example, in the following observation:

> When speaking of privacy, scholars at one end of the spectrum contend that privacy promotes or protects relationships, one's personhood and the creation of self, one's dignity, and even democracy and rejection of totalitarianism. At the other end of the spectrum, scholars dismiss privacy as simply protecting property interests, as promulgating subordination of, and violence to, women by men, or as promoting, or at least rewarding, fraud and deceit.[11]

The purpose of this section is to introduce the concept of privacy as a contested term and the privacy issues that arise in relation to the ubiquitous retention of the community's metadata. This section will begin by examining what privacy is and why it is important; it will then review the development of privacy literature over time as separated into three waves of discourse delineated by the prevailing privacy problem of the time. Finally, having established the paradigm for the current, third wave of privacy discourse, this section will examine metadata retention laws and conclude that, from a theoretical perspective, metadata retention, without due justification, breaches fundamental privacy rights.

---

[7] Macquarie Dictionary Online. *Privacy* (August 2016) Pan MacMillian Australia <https://www-macquariedictionary-com-au.simsrad.net.ocs.mq.edu.au/features/word/search/?word=privacy&search_word_type=Dictionary>.

[8] Oxford English Dictionary Online, Privacy (March 2016) Oxford University Press <http://www.oed.com/view/Entry/151596?redirectedFrom=privacy>.
Five additional definitions are offered, varying in currency, and collectively allude to notions of: 'privity', 'avoidance of publicity or display', 'protection from public knowledge or availability,' 'personal matters' and 'intimacy.'

[9] Warren and Brandeis, above n 1.

[10] Richard Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 562.

[11] Ibid 555-556.

B *Characterising 'Privacy' and its Significance*

The concept of privacy remains contested, with variations contingent on one's cultural background, economic status, access to technology, and the prevailing political climate.[12] The above quote from Bruyer aptly captures the array of scholarly interpretations as falling along one of two spectrums. While a dominant conception of privacy draws upon Western liberal values, privacy discourse has branched out to explore different perspectives. For instance, Fuchs advances an alternative socialist concept of privacy to challenge the prevailing 'liberal bias', arguing that privacy may not be a collective good at all times and that there are instances whereby privacy needs to be constrained.[13] Intercultural comparisons of privacy have also featured in these accounts, such as Capurro's study of Japanese and Western notions,[14] and Whitman's consideration of the 'transatlantic clash' between American and continental European approaches to the concept of privacy.[15] Despite reaching the same conclusion — that privacy warrants protection — the European approach emphasizes dignity ('the right to control your public image — rights to guarantee that people see you the way you want to be seen')[16] whereas the American tradition centres on liberty (the 'right to freedom from intrusions by the state, especially in one's own home').[17] Finally, a view that privacy is worth protecting engages debates relating to whether deontological or consequentialist approaches ought to be adopted.[18]

The conceptual difficulty in defining privacy has been well documented. The majority of sources discussing privacy commence with the same caveat on the lack of consensus – morally or legally. In 1873, Stephen advanced that 'to define the province of privacy distinctly is impossible'.[19] Similarly, in 'Understanding Privacy', Solove writes that privacy is a nebulous concept (one 'in disarray') intertwined with a range of related ideas: '(among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations'.[20] After referring to

[12] Trina Magi, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' (2011) 81(2) *The Library Quarterly* 187.
[13] Christian Fuchs, 'Towards an alternative concept of privacy' (2011) 9(4) *Journal of Information Communication and Ethics in Society* 220, 225.
[14] Rafael Capurro, 'Privacy. An intercultural perspective' (2005) 7(1) *Ethics and Information Technology* 37.
[15] James Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113(6) *Yale Law Journal* 1151, 1153.
[16] Ibid 1162.
[17] Ibid 1161.
[18] David Lindsay, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29(1) *Melbourne University Law Review* 131.
[19] Sir James Fitzjames Stephen, *Liberty, Equality, Fraternity* (first published 1873; Cambridge University Press, 1967) 160. Stephen went on however, to propose an impossibly broad 'description' of privacy as 'conduct which can be described as indecent': at 160.
[20] Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008) 1.

Miller,[21] Franzen,[22] Inness,[23] Gross,[24] Bennett[25] and Post,[26] Solove concludes that 'privacy seems to encompass everything, and therefore it appears to be nothing in itself'.[27]

According to Bendall, privacy has a long history in literature across cultures, from the Qur'an and the Bible, recognition in ancient China and classical Greece, as well as its characterisation under Jewish law as freedom from surveillance.[28] In the *Stanford Encyclopaedia of Philosophy*, DeCew traces the origins of the modern understanding of privacy to Aristotle's delineation between the 'public sphere of political activity' and the 'private sphere of domestic family life'.[29] Similarly, in *On Liberty* (1859), Mill spoke of the regulation of private conduct by public authority, thus continuing the language of the public/ private distinction.[30]

Privacy received much discussion over the years by way of consistent philosophical commentary until the 1890s; however, one particularly poignant statement appears in 1763 by United Kingdom MP William Pitt, 1st Earl of Chatham, who remarked:

> The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement.[31]

In this proclamation, Pitt reinforces the division between public and private and employs the threshold of one's home as a device to represent the importance of consent. It speaks to the inviolability of a person's home – the notion that persons or authorities lacking express or implied permission to enter a home are barred by law from doing so. Further, that even the lowliest person could refuse a King entry to their home demonstrates the importance with which this right was regarded. Moreover, it is possible to read the quote as an extended metaphor regarding an

[21] Ibid. See also: Arthur Miller, *The Assault on Privacy* (University of Michigan, 1971) 25: privacy is 'difficult to define because it is exasperatingly vague and evanescent'.
[22] Solove, above n 18. See also: Jonathan Franzen, *How to Be Alone* (Picador, 2003) 42. Franzen states 'privacy proves to be the Cheshire cat of values: not much substance, but a very winning smile'
[23] Solove, above n 18, 1-2. See also: Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press, 1992) 3: 'privacy is in a state of chaos'.
[24] Solove, above n 18, 1-2. See also: Hyman Gross, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34, 35: 'the concept of privacy is infected with pernicious ambiguities'.
[25] Solove, above n 18, 1-2. See also: Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992) 25: 'attempts to define the concept of 'privacy' have generally not met with any success'.
[26] Solove, above n 18, 1-2. See also: Robert Post, 'Three Concepts of Privacy' (2011) 89 *Georgetown Law Journal* 2087, 2087. Post noted that 'privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all'.
[27] Solove, above n 18, 7.
[28] Anthony Bendall, 'A Short History of the 'Right to Privacy'' (2009) 44(1) *Agora* 37, 37.
[29] Judith DeCew, 'Privacy' in Edward Zalta (ed), *Stanford Encyclopedia of Philosophy* (Stanford University, 2006) <http://plato.stanford.edu/entries/privacy/>.
[30] John Stuart Mill, *Utilitarianism, Liberty and Representative Government* (J.M. Dent & Sons Ltd, 1964) 76.
[31] William Pitt, *Speech on the Excise Bill*, House of Commons, Parliament of the United Kingdom (March 1763).

individual's rights against State intrusion, namely, where privacy provides an extension of the bodily integrity of a person.

Bruyer, quoting a Canadian Supreme Court decision of 1997,[32] states that 'the protection of privacy is a fundamental value of modern, democratic states'. Importantly for present purposes and in light of the discussion of metadata retention, government surveillance and intrusion into the private lives of individuals have been noted as leading to circumstances that are an antithesis to the principles of a liberal democracy. Privacy violations are said to lead to circumstances of self-censorship, to the inhibition of free speech, and the censoring of dissent to social norms.[33] Further, a paramount concern regarding privacy intrusion is that it has an inhibitory effect on individuality and breeds conformity though self-censorship.[34]

Equally, however, a degree intrusion into privacy is necessary for the safety and security of society. In this age of pervasive technology use, surveillance can act as both a deterrent to crime and significant investigatory tool in the hands of law enforcement. Nonetheless, pervasive surveillance or even the threat of pervasive surveillance can have negative effects upon the individual. In the late 18th century, Jeremy Bentham posited that the mere threat of surveillance of a person's actions has a chilling effect on behaviour, a phenomenon termed the Panoptic Effect after Bentham's architectural design for a prison called the Panopticon.[35] According to this design, the inmates' cells were arranged around a central tower; the guards could see into the prisoner's cells but the prisoners could not see the guards from their cells.[36] The prisoners would rationally assume that they were being surveilled and would moderate their behaviour even without any positive confirmation of the surveillance taking place.[37] In effect, the awareness of possible surveillance proves to be as inhibitory on an individual's behaviour as actual surveillance. This becomes an even more significant issue when everyone is subject to surveillance – criminals and innocents alike. Surveillance, as will be discussed further below, is a 'sweeping form of investigatory power'.[38] In the instance of government-mandated metadata retention, all persons within the territory of Australia are essentially under potential surveillance at all times regardless of any actual wrongdoing. This is incongruent with a society that prides itself on its respect for human rights and the dignity of the individual. The privacy problems arising out of the use of metadata to essentially enforce 'societal values' will be discussed in a latter part of this section following an examination of the evolution the concept of privacy over time.

---

[32] *Dagg v Canada (Minister of Finance)* [1997] 2 S.C.R. 403, 434 [65].
[33] Peter Swire, 'Financial Privacy and the Theory of High-Tech Government Surveillance' (1999) 77 *Washington University Law Quarterly* 461, 473.
[34] John Gilliom, *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy* (Chicago University Press, 2001) 3.
[35] David Lyons, *The Electronic Eye: The Right of Surveillance Society* (Polity Press, 1994) 62-67.
[36] Michel Foucault, *Discipline & Punish: The Birth of the Prison* (Vintage Books, 1995) 200 [trans of: *Surveiller et Punir* (first published 1975)].
[37] Lyon, above n 32, 63.
[38] Daniel Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 495.

II Privacy: Three Waves of Development

An overview of privacy literature of the last 130 years demonstrates that it has received academic treatment in three dominant waves. The First Wave began in 1890, heralded by Warren and Brandeis' seminal article *The Right to Privacy*.[39] The Second Wave came to the fore in the 1960s and 70s following the increased focus on human rights after the Second World War and driven by Prosser's *Privacy*[40] and Westin's *Privacy and Freedom.*[41] Banisar and Davies indicate that 'interest in the right of privacy increased in the 1960s and 1970s with the advent of IT'.[42] The Third Wave, which, arguably, continues today, proliferated in the 2000s with the works of writers including Banisar,[43] Bruyer,[44] and Solove driven by the explosion of developments in telecommunication technology and increased global interconnectedness.[45]

A *First Wave*

In what Elbridge referred to as 'one of the most brilliant excursions in the field of theoretical jurisprudence',[46] Warren and Brandeis advocated for legal recognition of privacy as a 'right to be let alone'.[47] While the authors are often credited with the advent of the phrase, Brandeis and Warren cite the nineteenth century judge and constitutional scholar Thomas Cooley as the originator.[48] As Bratman affirms, Brandeis and Warren viewed a legal right to privacy as the appropriate means to respond to the personal intrusions resulting from recent inventions of 'instantaneous photographs and newspaper enterprise[s]'.[49] The authors claimed that this incremental advancement in common law would be consistent with the development of privacy law that had already extended the protection afforded to persons and property., They were not arguing for a new right, but for the extension of an existing one.[50] A tort of invasion of privacy was advanced, with a number of caveats

---

[39] Warren and Brandeis, above n 1.
[40] Williams Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383.
[41] Alan Westin, *Privacy and Freedom* (Atheneum, 1967).
[42] David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18 *John Marshall Journal of Computer and Information Law* 1, 10.
[43] David Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments*, (5 May 2008) Privacy International <www.privacyinternational.org/survey/phr2000/overview.html>.
[44] Bruyer, above n 8.
[45] Solove, above n 18; Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087; Daniel Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477; Daniel Solove, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745.
[46] Elbridge Adams, 'The Right of Privacy, and its Relation to the Law of Libel' (1905) 39 *American Law Review* 37, 37.
[47] Warren and Brandeis, above n 1, 205.
[48] Thomas Cooley, *Cooley on Torts* (2nd ed, 1888) 29.
[49] Benjamin Bratman, 'Brandeis and Warren's *The Right to Privacy* and the Birth of the Right to Privacy' (2001-2002) 69 *Tennessee Law Review* 623, 630.
[50] Ibid 632; Warren and Brandeis, above n 1, 194-5.

on its scope: for example, it would not apply to matters of 'public or general interest'[51] or be actionable by individuals who had forsaken their right to exist without public scrutiny 'including candidates for, and holders of, public office and others'[52] Further, it would not cover privileged communications or cases where the individual aggrieved consented to publication, nor would truth or the absence of malice provide a viable defence.[53] In essence, the first wave of privacy advocated the protection of the person against unauthorised access; this included unauthorised publication of materials related to, about or belonging to a person.[54] The first wave can thus be characterised as the protection of the private persona of the individual.

B *Second Wave*

The second wave of privacy development resulted as a response to the Second World War. Following the end of the Second World War, human rights were a significant topic of discussion, including the international human right to privacy. At the time, the world was examining the idea of common humanity, especially in light of the atrocities then only recently committed. As such, the idea of a shared humanity and human dignity took prevalence and was articulated into a set of fundamental human rights shared by all by nature of their shared humanity. It was argued that the right to privacy underpins and allows for many other rights and freedoms to be exercised – such as freedom of religion and freedom of expression. Many of the atrocities perpetrated during the Second Word War were possible due to the extreme violations of individual privacy, and following the war, the protection of privacy was taken seriously in Germany and elsewhere around the world.[55] At the time, state constitutions protected the inviolability of the home and correspondence,[56] reflective of the privacy problems of the First Wave.

In 1960, Prosser reviewed over 300 privacy cases from the United States heard since Warren and Brandeis' seminal essay. He segmented the 'right to be let alone' into four disparate but related privacy torts: (1) intrusion upon a person's seclusion, solitude, or private affairs; (2) public disclosure of embarrassing facts; (3) publicity that places a person in a false light; and (4) appropriation of a person's name or likeness for the advantage of another.[57] One decade later and building upon Prosser's expanded understanding, Westin defined privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[58] Westin positions privacy as a fundamental element of a liberal

[51] Warren and Brandeis, above n 1, 214.
[52] Ibid 215.
[53] Ibid 216-18; Bratman, above n 27, 632.
[54] Warren and Brandeis, above n 1, 205.
[55] Thomas Shaw, *World War II Law and Lawyers: Issues, Cases, and Characters* (ABA Book Publishing, 2013).
[56] Oliver Digglemann and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441, 441.
[57] Prosser, above n 37, 389.
[58] Westin, above n 38.

democracy, promoting freedom of association, government accountability through the protection of the secret ballot and press privilege, and protection from improper intrusion by law enforcement into the lives of civilians, for example, in relation to search and seizure:

> A balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life.[59]

In 1975, Altman described privacy succinctly as 'selective control of access to the self'.[60] In a more widely cited analysis from 1980, Gavison[61] attempted to present privacy as 'a distinct and coherent concept'[62] and identified two important privacy questions: what is the status of privacy (does it exist as 'a situation, a right, a claim, a form of control, a value?'),[63] and what are the characteristics of privacy (for instance, in relation to information, autonomy, personal identity, physical access, and so on).[64] As to the former, Gavison preferred a 'neutral concept of privacy' as 'a situation of an individual vis-à-vis others, or as a condition of life'.[65] As to the latter, Gavison found privacy to be 'a complex' of 'three independent and irreducible elements': secrecy (the extent to which an individual is known), anonymity (the extent to which an individual is the subject of attention) and solitude (the extent to which others have physical access to an individual).[66] The second wave of privacy discourse extended the discourse of the first wave by incorporating the right of the individual to control access to oneself and to limit what is known about them by others

C Third Wave

The Third Wave of literature was driven by an explosion of telecommunications and computing technology in the 1990s and into the 21st century. Scholars continued their efforts to construct all-encompassing definitions of privacy that would be an effective response to these developments. For example, Simmel states:

> Privacy is a concept related to solitude, secrecy, and autonomy, but it is not synonymous with these terms; for beyond the purely descriptive aspects of privacy as isolation from the company, the curiosity, and the influence of others, privacy implies a normative element: the right to exclusive control of access to private realms… the right to privacy asserts the sacredness of the person;… any invasion of privacy constitutes an offence against the rights of the personality – against individuality, dignity, and freedom.[67]

---

[59] Ibid 24.
[60] Irwin Altman, *The Environment and Social Behaviour: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole Publishing Co, 1975) 18.
[61] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89(3) *Yale Law Journal* 421.
[62] Ibid 423.
[63] Ibid 424.
[64] Ibid.
[65] Ibid 425
[66] Ibid 429-434.
[67] Arnold Simmel, 'Privacy' (1968) 12 *International Encyclopedia of the Social Sciences* 480, 482.

The authors of the Third Wave such as Banisar, Bruyer, and Solove, saw a movement away from 'essentialism' (that is, viewing privacy as a single universal thing). The discussion of what is privacy and what is privacy intrusion became more nuanced over time and across the progression of the predominant waves; however, this also resulted in more divergent concepts of privacy depending on the author. Solove likens the term 'privacy' to the term 'animal' – both are general terms that people would instinctively understand without having to visualise specifically. However, when considering specifics, different people think of different aspects of the general term – a dog and a cat may both be animals but are very different; the same can be said of privacy in that different actions that infringe upon privacy, have different causes and impacts.[68] A similarly frustrating definitional struggle is evident in attempts to define the term 'terrorism'; it is perhaps of interest to note that the adage 'one man's terrorist is another man's freedom fighter' has come to be called 'the relativity definition'.[69] Simply put, having a varied discussion on the topic of privacy and attempting to formulate a single, coherent definition has over time led to a dilution of meaning of the concept as many authors suggest their own, competing versions of the concept of privacy.

Two examples of privacy revisionism from this period are Post's *Three Concepts of Privacy*,[70] and Bruyer's *Privacy: A Review and Critique of the Literature* as published in the Alberta Law Review Special Issue on Privacy Law.[71] Post compares and contrasts three concepts of privacy - the first connects privacy to the creation of knowledge; the second connects privacy to dignity; and the third connects privacy to freedom.[72] In brief, Post found that the first concept 'should not be understood as a question of privacy', the second is 'helpful to apprehending privacy, but … it should focus our attention primarily upon forms of social structure,' and the third is 'best conceived as an argument for liberal limitations on government regulation'.[73] Bruyer critiques the 'intuitive approach' employed in privacy literature where there is an assumption that 'we all approach privacy with a common understanding of the concept, or concepts, that the term privacy expresses'.[74] In addition, Bruyer rejects the paradigm of 'privacy as liberty' and instead suggests that it ought to be conceived instead as an issue of equality. Moreover, Bruyer critiques the earlier conceptions of privacy – particularly in terms of the arbitrary delineations of the application of privacy protection depending on each author's understanding of the concept of privacy. His conclusion is that earlier conceptions of privacy were both too narrow and too broad to be useful in offering privacy protection.[75] Instead, Bruyer's central thesis for conceptual reform is that 'the focus should shift away from conceptualising privacy

[68] Solove, above n 35. 486.
[69] Bruce Hoffman, *Insider Terrorism* (Victor Gollancz, 1998) 131.
[70] Robert Post, 'Three Concepts of Privacy' (2011) 89 *Georgetown Law Journal* 2087.
[71] Bruyer, above n 8.
[72] Post, above n 67, 2087.
[73] Ibid.
[74] Bruyer, above n 8, 553.
[75] Ibid 558

as a prerequisite for preventing invasions of various liberty interests to one of 'maintaining conditions' that will make the exercise of those liberties possible.[76]

In a similar manner, rather than offering a universal definition of privacy, Banisar and Davies adopt the approach of dissecting the different facets of privacy, distinguishing between four typologies: territorial privacy, privacy of communication, bodily privacy, and information privacy.[77] This analysis has frequently been cited in the literature and breaks down as follows:

(a) Territorial privacy: concerning the setting of limitations on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.
(b) Privacy of communication: covering the security of privacy of mail, telephones, email and other forms of communication.
(c) Bodily privacy: regarding the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches.
(d) Information privacy: involving the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records, also known as 'data protection'.[78]

This movement away from defining privacy as a single concept was observed by Daniel Solove in his acclaimed body of work. Solove explicitly states that 'in the 20th century, essentialism was rejected as a useful means of defining words or concepts', and further, that examining 'family resemblances' between related concepts in particular contexts forms a more viable basis for the determination.[79] Within the context of privacy, he observes that the debate about the meaning of privacy has faltered due to this preoccupation with isolating a 'core meaning'[80] as results are 'too broad and vague to be useful in addressing concrete issues'.[81] Solove identifies six general aspects of privacy that require protection: '(1) the right to be let alone, (2) the ability to limit access to the self by others, (3) secrecy or concealment of certain matters, (4) the ability to control information about oneself, (5) the protection of one's personhood, individuality and dignity, and (6) control over one's intimate relationships or aspects of life'.[82] Based on this analysis, he also identifies four broad groupings of activities that attract potential privacy concerns: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion (meaning the unauthorised access to the

[76] Ibid 587.
[77] Banisar and Davies, above n 39.
[78] Ibid 6.
[79] Solove, above n 35, 486.
[80] Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1096-9.
[81] Solove, above n 35, 485.
[82] Solove, above n 77, 1092.

self and to personal information).[83] As will be discussed in the subsequent section, the retention of individual metadata impacts upon all four of Solove's identified categories of privacy problems.

III Privacy, Metadata Retention and Solove's Taxonomy

Technological developments have made access to information about the individual more widely available and of greater scope. From the First Wave's consideration of newspapers printing information without consent, the Third Wave deals with information that is widely available on the internet – whether intentionally shared (think images posted to social media) to information that is derived (think social media using user information to target advertising to users). The scope of information about an individual available to interested persons in the Third Wave of privacy concern is vast. Solove's Taxonomy of Privacy Problems ('**the TPPs**') attempts to categorise the many modern threats to individual privacy; Solove articulated the TPPs to account for the diverse nature of definitions offered in previous iterations of privacy research. In Solove's view, 'there is no one answer [to privacy,] but a variety of answers depending on a variety of factors'.[84] Solove's TPPs, grouped into four categories, are further subdivided into groupings showing related privacy problems.[85] The collection of individual's metadata has the potential to trigger concerns related to a range of privacy problems identified by Solove – particularly, Surveillance, Aggregation, Identification, Insecurity, Secondary Use, Disclosure, and Intrusion. These are discussed below, first noting the categories, and then identifying the specific privacy problems impacted by metadata retention.

A *Information Collection*

Whether it is made public or not, the process of information collection creates privacy problems, and therefore, harm.[86]

1 *Surveillance*

Whether visual, audio or electronic, surveillance has long been seen to be a privacy issue. Violations of a person's physical privacy in instances where they can reasonably expect not to be seen by outsiders is a common element of criminal law.[87] Surveillance, when done in a continuous or ubiquitous manner, can have problematic effects.[88] Broadly speaking, ubiquitous surveillance can lead to self-censorship and inhibition of personal expression.[89] Pervasive and ubiquitous monitoring of

[83] Solove, above n 18, 10-11.
[84] Solove, above n 77, 1098-1099.
[85] Solove, above n 18, 10-11.
[86] Solove, above n 35, 491.
[87] For example, see: *Crimes Act 1900* (NSW) ss 91I-91M, 547C.
[88] Solove, above n 35, 493.
[89] Swire, above n 30, 473; for a discussion concerning the impact of internet surveillance on human behaviour, see also, Jonathan Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) *Berkeley Technology Law Review* 117; and Antti Oulasvirta et al, 'Long-Term Effects of Ubiquitous Surveillance in the

behaviour inclines an individual to conformity with societal expectations; 'monitoring constrains the acceptable spectrum of behaviour'.[90] Further, Gilliom observes:

> Surveillance of human behaviour is in place to control human behaviour, whether by limiting access to programs or institutions, monitoring and affecting behaviour within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance.[91]

However, surveillance can serve as a deterrent to crime and serve an investigatory function after a crime has been committed.[92] And yet, surveillance is a deeply intrusive power of investigation as it 'records behaviour and social interaction', amongst other activities.[93] If surveilled for long enough, a person might eventually be found to be engaging in some form of immoral or illegal activity.[94] While it may appear that catching a person engaging in illegal activity justifies the surveillance, not all criminal activity, morally or legally, justifies intrusive surveillance. Moreover, activity that is merely immoral or that does not accord with society standards can be caught up in a surveillance dragnet, that can be later used to blackmail or discredit a person; for example, consider the Federal Bureau of Investigation surveillance of Dr Martin Luther King Jr, the purpose of which was to uncover material that could have been used to damage Dr King politically. Indeed, it appears the FBI has a long history of politically and religiously motivated surveillance, as uncovered during a US Congressional investigation into the Dr King matter.[95]

The metadata retention legislation under consideration in this thesis mandates the retention of personal data for a period of two years.[96] During this time, societal standards may change; new laws may be enacted to criminalise behaviour that was legal at the beginning of the two year period. Having the data stored would expose persons to the risk of prosecution for past behaviour because, while there is a presumption against retrospectivity of legislation, it is not absolute. The mere possibility of the misuse or secondary use of the stored data is reason enough for concern. The fact that the storage of metadata is mandated throughout Australia, regardless of whether an individual is subject to police investigation or not, is further reason for consternation. As noted by Frank Donner – '[t]he selection of a target [for surveillance] embodies a judgment of deviance from the dominant

---

Home' (Paper presented at the 14th International Conference on Ubiquitous Computing, Pittsburgh, USA, 05 to 08 September 2012).

[90] Julie Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373, 1496.

[91] Gilliom, above n 31, 3.

[92] Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random house, 2004) 36.

[93] Solove, above n 35, 495.

[94] Ibid 496.

[95] United States Congress Select Committee, *Intelligence Activities and the Rights of Americans, Book II: Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Congress (1976) 7.

[96] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187C.

political culture';[97] it would thus appear that with the enactment of the metadata retention laws, the Government views anyone in Australia as potentially deviant.

B *Information Processing*

Referring to the use, storage, and manipulation of stored information once it has been collected. This also involves drawing additional information, the making of deductions on the basis of collected information and other consolidation of stored data.[98]

1 *Aggregation*

Aggregation refers to the collation and analysis of disparate sources of information regarding an individual.[99] Individually, each bit of information is not very telling, however, when combined, information reveals facts and conclusions about the person that that could not have been foreseen from the isolated data that was originally collected.[100] This is particularly indicative of the privacy problems that arise in the third wave discussed above – technologically-assisted collection and analysis of information—such as that allowed by the metadata retention regime in Australian— can result in substantial privacy problems. While considering the issue of proprietary interests in collated and aggregated information about a person is outside the scope of this research, this process reveals facets of private lives; apart from allowing inferences to be drawn about an individual, there is no guarantee that the inferences are complete or accurate, and this has the potential for distortion and inequity.[101] The retention of individual's metadata, for instance, may tell of a website that was visited; however, there is no scope for allowing for motivation and the causal 'why', and there is no way to evidence who was operating the device at the time. The result is a potential misinterpretation of data when it is devoid of context.

2 *Identification*

Identification refers to connecting available information about individuals to their personal identity.[102] Identification of persons, no matter how anonymised the information, is possible if there is sufficient cross-correlation between data sets.[103] With sufficient information within and cross-referenceable between databases, the notion of anonymity evaporates – individuals can be identified with near

---

[97] Frank Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System* (Knopf, 1983) 3.
[98] Solove, above n 35, 504-505.
[99] Solove, above n 35, 507.
[100] Cohen, above n 87, 1398.
[101] Jeff Smith, *Managing Privacy: Information Technology and Corporate America* (Southern Economic Association, 1994) 121.
[102] Roger Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7 *Information Technology & People* 6, 8.
[103] Yves-Alexandre de Montjeye et al, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347(6221) *Science* 536, 536-537.

perfect accuracy.[104] Solove states that aggregation of data creates 'a digital person, a portrait composed of information fragments combined together';[105] identification then links the digital person directly to the persona of the individual in the real world.[106] Historically, identification has been used by governments to seek out dissidents, radicals and others in society whose views may be contrary to or, as noted above, 'deviant from the dominant political culture'. [107] As such, the government-mandated collection and storage of metadata enables the government to utilise stored information to not only draw conclusions about the lives of individuals, but also to identify who those individuals are in the real world. This is accomplished by obtaining metadata from disparate sources and cross-referencing available information.

3 *Insecurity*

Insecurity refers to the way in which the various pieces of information, physical and digital, can be used to undermine a person's sense of privacy and security.[108] While Solove discusses Insecurity in relation to identity theft, for present purposes, unauthorised access, use, or disclosure of information can be suggested as substitutes. Related to Aggregation and Identification, Insecurity is primarily caused by the way that personal information is collected, handled, and secured.[109] With regard to metadata, the potential of unauthorised access to such a substantial trove of personal information is a valid reason to feel insecure.

4 *Secondary Use*

Secondary use refers to the use of information collected for one purpose being used for other purposes, often in ways to which the individual whose information was collected did not consent.[110] Essentially, secondary use involves the individual, whose information was collected, losing control over how the information is used and for what purpose. As will be discussed in a later section, the collection of metadata creates a secondary use privacy problem as data being collected for billing and other purposes by telecommunication providers, is being repurposed for to investigate offences ranging from threats to national security and serious criminal offence, to minor traffic and administrative offences, while also being used to potentially target journalists and whistleblowers.[111]

---

[104] Ibid 538.
[105] Solove, above n 35, 514.
[106] Ibid.
[107] Smith, above n 98.
[108] Solove, above n 35, 515.
[109] Ibid.
[110] Ibid 521.
[111] A specific instance took place in Australia earlier this year when a journalists' metadata was used to investigate a whistleblower that leaked documents that were embarrassing to the government.

C *Information Dissemination*

The next step in privacy intrusion, dissemination, involves the spread of information about the person beyond the control or consent of the individual.[112]

1 *Disclosure*

This refers back to the meaning of privacy articulated in the First Wave – that of disclosure of private information about the person that is not of concern to the public. This refers to the protection of personal against records about the individual, such as government records, medical records and the like.[113] Importantly, the protection against disclosure is the protection against personal information being used maliciously against a person, whether by governments or other individuals.[114] As will be discussed shortly, personal information is often subject to unauthorised disclosure – whether by government agencies or by other non-government entities or individuals; this may happen inadvertently or maliciously, and the retention of metadata exacerbates the threat.

D *Invasion*

Invasion directly flows from the above privacy problems and leads to impacts upon the decisions made by the individual once their privacy had previously been compromised.[115]

1 *Intrusion*

The concept of intrusion refers to privacy problems that were commonly associated with privacy problems of the First and Second Waves – trespass upon private property; unauthorised viewing of correspondence or other secure items; and the intrusion upon a person's solitude,[116] these are all examples of Intrusion. Intrusion is related to the gathering and the ascertaining of information about the person, with the intent to somehow invade the persons' sense of seclusion and enjoyment of their space.[117] Relevant to several of the items listed, Intrusion can occur when aggregated information is used to identify a person, or when information about the person is used in a way to create feelings of insecurity. Considering the examination of Solove's TPPs above that identify the causes of privacy concern in respect to metadata retention, the next section seeks to identify the standard of required privacy protection at international law.

---

[112] Solove, above ne 35, 523.
[113] Ibid 527-528.
[114] Eugene Volokh, 'Freedom of Speech and information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You' (2000) 52 *Stanford Law Review* 1049, 1050-1051.
[115] Solove, above n 35, 548.
[116] Ibid 549.
[117] Ibid 549-550.

IV Privacy in International Law

The purpose of this section is to introduce the broad framework of international human rights as they pertain to the right to privacy. This section will briefly introduce the sources of the international legal right to privacy and the relevant legal tests by which compliance by states may be measured. The evaluation of the tests and their application to Australia's metadata retention law will happen in a latter section. The recognition of human rights has a long history in international law, however, this thesis will focus on the modern era of human rights, specifically from the turn of the 20th century to the present day, particularly the developments following the end of the Second Word War. Following the cessation of conflict in 1945, the United Nations' Charter was signed; in the Preamble to the Charter, the signatory states expressed the need to prevent and control international armed conflict, and affirmed the fundamental and universal value of human rights.[118] The focus at the time was an examination of what it meant to be human and a recognition of a shared humanity. The aim was to ensure that through the recognition of fundamental human rights shared by all, the events of the Second World War would not be repeated.

In furtherance of the goal to 'reaffirm faith in fundamental human rights',[119] the General Assembly of the United Nations ('**UN**') adopted the *Universal Declaration of Human Rights* in 1948 ('**UDHR**').[120] One of the stated aims of the UDHR is to recognise 'the inherent dignity and … the equal and inalienable rights of all members of the human family'.[121] This document served as a foundation for the development of international human rights law in subsequent decades, becoming an integral text defining the first and subsequent generations of human rights.

A *International Bill of Human Rights*

What resulted was the creation of an International Bill of Human Rights ('**IBHR**') comprised of three seminal instruments: the *Universal Declaration of Human Rights*; the ICCPR; and the *International Covenant on Economic, Social and Cultural Rights* ('**ICESCR'**).[122] The UDHR and the ICCPR represent the first generation of human rights, comprising the protection of civil and political rights; the first generation of human rights focuses on a person's freedom to participate in the civil and political life of a nation. Both the UDHR and the ICCPR include provisions for protecting the private life of the individual against unwarranted intrusions by the state and both of these documents will be discussed

[118] *Charter of the United Nations*, Preamble.
[119] Ibid.
[120] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) ('*UDHR*').
[121] Ibid Preamble.
[122] *International Covenant on Economic, Social and Cutural Rights*, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 03 January 1966).

in greater detail, together with relevant regional instruments, with a focus on the extent to which individual privacy is protected under international law.

The UDHR does not dictate a hierarchy of rights,[123] however, jurisprudentially, civil and political rights have been categorised as the 'first generation' of human rights whereas economic, social and cultural rights are considered 'second generation' rights.[124] As concerns about privacy fall within the scope of civil and political rights, the following discussion will concentrate primarily on the first generation rights set out in the ICCPR. This instrument is also legally binding upon its state parties, which include Australia.

1 *Universal Declaration of Human Rights*

The UDHR was adopted on 10 December 1948 at Paris by the United Nation's General Assembly ('**UNGA**'). While not intended to be a binding legal instrument,[125] the UDHR was intended to serve as a 'common standard […] for all peoples and for all nations'.[126] As such, when read as a whole and together with the UN Charter, the UDHR urges Member states of the UN to undertake the protection of human rights in an aspirational manner.[127] The UDHR was adopted with the support of 48 states, eight abstentions, and with no dissentions.[128] Article 12 of the UDHR specifies that that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'[129] The UDHR has achieved unanimous recognition as a foundational document of the UN, representing the values of the organisation and what it is seeking to achieve and promote. Although the UDHR itself was not legally binding upon states, some provisions have over time become part of customary international law.

2 *International Covenant on Civil and Political Rights*

The ICCPR was opened for signature in 1966 and entered into force in 1976.[130] As of 2017, there are 169 state parties to the Covenant. Having been ratified on 13 August 1980, the ICCPR is legally binding upon Australia. The purpose of the ICCPR was to implement an international agreement that, unlike

---

[123] Hugo Stoke and Arne Tostensen (eds), *Human Rights in Development Yearbook 1999/2000: The Millennium Edition* (Kluwer Law International, 2001) 76. However, while not hierarchical in nature, the structure of the UDHR was carefully constructed in order to produce an effect of progressing from fundamental to more broad-scoped rights and freedoms. See also: Mary Ann Glendon, 'The Rule of Law in the Universal Declaration of Human Rights' (2004) 2(1) *Northwest Journal of International Human Rights* 1, 3.

[124] Martin Dixon, *Textbook on International Law* (Oxford University Press, 7th ed. 2013) 345.

[125] Mary Ann Glendon, 'Knowing the Universal Declaration of Human Rights' (1998) 73(5) *Notre Dame Law Review* 1153, 1164.

[126] *UDHR*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) Preamble.

[127] Mary Ann Glendon, 'The Rule of Law in the Universal Declaration of Human Rights' (2004) 2(1) *Northwest Journal of International Human Rights* 1, 10.

[128] United Nations, *History of the Document* <http://www.un.org/en/sections/universal-declaration/history-document/index.html>.

[129] *UDHR*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 12.

[130] *ICCPR*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

the UDHR, would be legally binding upon states once they signed and ratified or acceded. States party to the ICCPR are obliged to implement the Covenant; however, as will be discussed in greater detail below, article 2.2 allows states to 'adopt such laws or other measures as may be necessary to give effect to the rights' contained in the Covenant. This allows for a broad range of measures by which the protections under the ICCPR may be implemented.

The ICCPR includes a range of monitoring and enforcement mechanisms; article 41, which allows for a state party to the Convention, upon a reciprocal declaration of recognition of competence of the UN Human Rights Committee, to bring a complaint to the Committee regarding the actions of another state party. Subject to the general principles of international law, including the requirement of exhaustion of local remedies, the Committee may aid the parties to negotiate an outcome; and if an outcome cannot be negotiated, the Committee may conciliate the matter. The outcomes of the state to state Committee findings are not binding and it is important to note that this procedure has never been used by one state to bring a complaint against another state. As it stands, the ICCPR itself has no provision for individuals to bring complaints directly to the Commission regarding the actions (or inactions) of state Parties. This limitation was remedied by the *Optional Protocol to the International Covenant on Civil and Political Rights*.[131] The *Optional Protocol* allows individuals subject to the jurisdiction of a state party[132] to lodge complaints directly to the Human Rights Committee; to date, there are 116 state Parties to the Optional Protocol. An additional method of ensuring compliance with the ICCPR is a mandatory reporting procedure enshrined in article 40. Under article 40, state Parties are required to submit progress reports on measures undertaken to ensure protection of rights guaranteed under the ICCPR whenever the Human Rights Committee so requests.

B *Article 17 of the International Covenant on Civil and Political Rights*

Article 17 sets out the protection of the fundamental human right to privacy and represents a legally binding successor to article 12 of the UDHR, but is broader in scope and is subject to the monitoring and enforcement mechanisms found in articles 40 and 41 of the ICCPR and the Optional Protocol.[133]

Article 17 of the ICCPR, states that:

1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour or reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[134]

[131] *Optional Protocol on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 302 (entered into force 23 March 1976) ('*Optional Protocol to the ICCPR*').
[132] Ibid art 1.
[133] The development of international law took place when the ICCPR entered into force in 1976. The ICCPR largely repeats the content of the UDHR but the key difference is in the fact that the ICCPR is binding upon states parties. Australia is a party to the ICCPR and has made any reservations nor declarations in respect of article 17.
[134] *ICCPR*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

The protection of privacy under article 17 of the ICCPR has been in the international legal spotlight in recent years largely due to the unprecedented capabilities of states to monitor the electronic and technological lives of those living within their territory and beyond. In 2013, the United Nations' General Assembly adopted a resolution entitled *The Right to Privacy in the Digital Age*.[135] The purpose of this resolution was to reaffirm the fundamental rights and freedoms enshrined in the IBHR, but further – to note that the rapidly evolving information and telecommunication technology enhances the capability of governments to 'undertake surveillance, interception and data collection',[136] which may lead to violations and abuse of human rights, particularly the right to privacy under article 12 of the UDHR and article 17 of the ICCPR. The Resolution further calls on all states to respect privacy in the context of digital communication and to ensure that adequate protections are enshrined in national legislation. This Resolution is indicative of the importance of the subject matter that is under discussion in this dissertation; the UN, through its organs, has been leading the dialogue recently and the work of these organs will be referred to in order to illustrate the key issues in this international debate.

1 *Unlawful and Arbitrary Interference with Privacy*

In 1988, the UN Human Rights Committee ('**UNHRC**') published *General Comment 16* on the topic of the interpretation of article 17 of the ICCPR.[137] In *General Comment 16*, the UNHRC offered commentary on the various aspects of the right to privacy, stating that governments should only 'be able to call for such information relating to an individual's private life the knowledge of which is *essential* in the interests of society' [emphasis added].[138] Further, the UNHRC directed that the protection of the individual's right to privacy must be provided for in the state's legislation.[139]

(a) Meaning of 'Unlawful'

General Comment 16 states that the term 'unlawful' suggested that no interference with privacy may take place 'except in cases envisaged by the law. Interference authorised by States can only take place on the basis of the law, which itself must comply with the provisions, aims and objectives of the [ICCPR]'.[140] In other words, and as pointed out by the Office of the United Nation's High Commissioner for Human Rights, 'interference that is permissible under national law may nonetheless be 'unlawful'

[135] *The Right to Privacy in the Digital Age*, GA Res 68/167, UN GAOR, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013).
[136] Ibid 1.
[137] Human Rights Committee, *CCPR General Comment 16: article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc HRI/GEN/1/Rev.1 (8 April 1988) ('*General Comment 16*').
[138] Ibid [7].
[139] Ibid [2]. The wording of this requirement states: 'it is precisely in State legislation above all that provisions must be made for the protection of the right set forth by [article 17]'.
[140] Human Rights Committee, *General Comment 16*, UN Doc HRI/GEN/1/Rev.1 (8 April 1988) [3].

if the national law is in conflict with the provisions of the [ICCPR]'.[141] Thus, for privacy limitations to be legal under international law, the limitation must be done on the basis of publicly accessible law that must comply with the state's constitutional regime and relevant international legal principles.[142]

The 'Accessibility' of any given law that seeks to infringe privacy, particularly in relation to communications and metadata 'requires not only that the law be published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct';[143] further, concerning any interference with the right to privacy under article 17 of the ICCPR, the state must ensure that the authorising laws:

1. Are publicly accessible;
2. Contain provisions that ensure that collection of, and access to, and use of communications data are tailored to specific legitimate aims;
3. Are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedure for authorising, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and
4. Provide for effective safeguard against abuse.[144]

To that end, paragraph 2 of article 17 of the ICCPR provides that states must ensure the protection of the law against unlawful or arbitrary interference. The notion of 'protection of the law' is interpreted as meaning procedural safeguards, and adequately funded institutional arrangements to allow for adequate oversight of infringing activities.[145] Thus, there must be competent and well-resourced administrative bodies that undertake the task of overseeing activities that infringe the right to privacy and per paragraph 3 of article 2 of the ICCPR, there must be a procedure in place to ensure that adequate remedies are available in instances where violations have been identified. The investigations of alleged breaches must be impartial, prompt and thorough, and following democratic principles of due process and the rule of law, backed by judicial authority. Finally, for a remedy to be considered effective, it must be able to end the violation, once proven; those tasked to investigate

[141] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 7 [21].
[142] Martin Sheinin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, 14th sess, Agenda Item 3, UN Doc A/HRC/14/46 (17 May 2010) Annex.
[143] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) 10.
[144] Ibid. Also discussed is the fact that the requirement for accessibility and having publicly accessible laws necessarily negates the possibility of secret laws, secret interpretations or secret judicial decisions. Any excessive discretion given to organisations with limited public accountability or disclosure procedures will not meet the required threshold of lawful interference. This is particularly relevant to the question of metadata retention as it does not easily lend itself to understanding with any degree of clarity how and in what circumstances the laws may be applied.
[145] Ibid 12-13.

potential violations must have sufficient expertise in the subject matter, have unfettered access to all relevant material and the capacity to issue binding orders.[146]

(b) Meaning of 'Arbitrary'

The right to privacy in international law is not absolute – it is a qualified right that may be interfered with under specific circumstances. These circumstances must weigh individual privacy against consideration of the essential interests of society broadly.[147] Thus, under the terms and interpretation of article 17 of the ICCPR, certain limitations and intrusions upon individual privacy are permitted – as long as they are not arbitrary in scope. Paragraph 4 of *General Comment 16* notes that government interference in the private lives of individuals may be deemed to be arbitrary within the meaning of article 17 even if the interference is conducted within the bounds of the domestic law of the state.[148] Even if the action is 'legal' in the sense that it has the status of domestic law, the action may still be arbitrary if it does not have a legitimate aim, is not necessary to achieve that aim, or is not proportionate to the goals that are sought to be achieved.[149]

(i) Necessity, Legitimacy and Proportionality

The requirement for necessity, legitimacy and proportionality in establishing principles of permitted interference is to ensure that such interference is reasonable, not arbitrary or unlawful. The concept of reasonableness was interpreted by the Human Rights Committee to indicate 'any interference with privacy must be proportionate to the end sought and be necessary in the circumstances of any given case'.[150] With regard to what constitutes arbitrariness, the International Court of Justice considered the question and proclaimed that 'arbitrariness is not so much something opposed to a rule of law, as something opposed to the rule of law…It is the wilful disregard of due process of the law, an act which shocks, or at least surprises, a sense of judicial propriety'.[151] It was later noted that what constitutes arbitrary conduct was not easily defined particularly in relation to human rights, however, the elements of 'injustice, unpredictability, unreasonableness, capriciousness, disproportionality and a lack of due process' were all identified as being indicative of arbitrary conduct.[152]

The framework of article 17 of the ICCPR is such that, as noted, it allows for necessary, legitimate and proportionate restrictions to the right of privacy. The restrictions are allowed by way of lawful and permitted limitations. However, while surrounding articles such as 18 and 19 outline a test for permitted limitations, article 17 lacks this express test. In examining this issue, the Special Rapporteur

---

[146] Ibid.
[147] Human Rights Committee, *General Comment 16*, UN Doc HRI/GEN/1/Rev.1 (8 April 1988) [7].
[148] Ibid [4].
[149] Navi Pillay, 'Right to Privacy in the Digital Age' (Speech delivered at the Expert Seminar of the UN Human Rights Council, Palais des Nations, Geneva, 24 February 2014).
[150] Human Rights Committee, *Views: Communication No 488/1992*, 50th sess, UN Doc CCPR/C/50/D/1992 (31 March 1994) [8.3].
[151] *Elettronica Sicula SpA (ELSI) (United states of America v Italy) (Judgment)* [1989] ICJ Rep 15, 65.
[152] Manfred Nowak, *UN Convention on Civil and Political Rights: CCPR Commentary* (N.P. Engel, 1993) 173.

on the Promotion and Protection of the Right to Freedom of Opinion and Expression noted that given the nature of the rights enshrined in the Covenant, the right to privacy should be interpreted as containing elements of a permissible limitation in the same vein as that described for article 12 that deals with freedom of movement.[153] As such, the test that will be applied to determine whether the restrictions placed upon the right to privacy under Australia's metadata retention regime are arbitrary nor unlawful, are whether the law serves a legitimate aim, whether it is effective and necessary at achieving that aim, and whether the law is proportionate in terms of its impact on individual privacy.

V METADATA RETENTION IN AUSTRALIA

In 1979, Australian Federal Parliament enacted legislation that allowed for the interception of communications, being defined as guided and unguided electromagnetic energy, passing over a telecommunications system.[154] As at 30 September 1992, its purpose was to 'prohibit the interception of telecommunications except where authorised in special circumstances or for the purposes of tracing the location of callers in emergencies, and for related purposes'.[155] Over time, the legislation dealing with authorised and unauthorised interception of telecommunications evolved to incorporate further amendments with respect to changing technologies and also to take account of a growing apprehension of intrusions into the privacy of the individual, both by state and non-state actors. This legislation, and other issues regarding the relationship between privacy, technology, and law enforcement were given prominence in 2008 with the publication of the Australian Law Reform Commission Report relating to individual privacy;[156] it is an issue that continues to be debated as seen during the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). It is worth noting that legislative recognition of privacy interests has developed in parallel with common law and that has left the question of the right to privacy in Australia subject to parliamentary development. A brief examination of the history of common law recognition of privacy in Australia is annexed hereto and marked Annexure A.

A *2008 Law Reform Commission Report*

In May 2008, the Australian Law Reform Commission ('**the Commission**') released a report considering Australian privacy law. The Terms of Reference for the Commission specifically included the '[r]apid advances in information, communication, storage, surveillance and other relevant

[153] See: Human Rights Committee, *General Comment 12: Freedom of Movement (Art 12)*, UN Doc CCPR/C/21/Rev.1/Add.9 (18 October 1999) [11]: states are authorised to restrict the right only in exceptional circumstances; [12]: the law must establish the circumstanced under which the right may be limited; [13]: the restrictions must not 'impair the essence of the right'; [14]: a legitimate aim is insufficient, necessity is a required element; and [15]: the principle of proportionality applies to any limitation both in how the law is framed, but also how it is applied by administrative authorities and interpreted by judicial authorities.
[154] *Telecommunications (Interception) Act 1979* (Cth) s 6.
[155] Ibid Long Title.
[156] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008).

technologies' and the 'possible changing community perceptions of privacy' to be considered in its review.[157] The Commission noted that the legislation allowing for access to telecommunications data (herein referred to as 'metadata'), the TIA Act, does not set out a definition of the term.[158] In 2007 when the TIA Act was amended to introduce provisions regulating access to metadata, the Explanatory Memorandum provided that metadata is:

> [I]nformation about a telecommunication, but does not include the content or substance of the communication. [Metadata] is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.
>
> For telephone-based communications, [metadata] includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, [metadata] includes the Internet Protocol (IP) address used for the session and start and finish time of each session.[159]

The Commission formed the view that the term metadata should not be defined under the TIA Act'to enable the legislation to remain technology neutral so that it can be applied to new developments in technology without the need for amendment' and to ensure a consistent approach across the TIA Act, the *Telecommunications Act 1997* (Cth) ('**Telecommunications Act**') and the *Privacy Act 1988* (Cth) ('**Privacy Act**').[160] However, the Commission further noted that given the '[p]rovision of this information...is a significant invasion of privacy',[161] more detailed guidance as to what falls within the ambit of metadata should be provided to intelligence and law enforcement agencies.

B *2013 PJCIS Report*

The report of the 2013 Pariamentary Joint Committee on Intelligence and Security ('**2013 PJCIS Inquiry**') was prepared at the request of the Federal Attorney-General based on a Terms of Reference containing 44 separate items of inquiry,[162] which dealt with, *inter alia*, the need to strengthen privacy protection[163] and the possibility of implementing a data retention regime.[164] From the outset, the 2013 PJCIS Inquiry noted that the data retention scheme sought by the Government (modelled on the European Union data retention Directive 2006/24/EC)[165] took up the majority of the Inquiry's time.[166] A full section of the Inquiry's five-section report is devoted to examining the issue of a metadata retention regime, with the Inquiry noting that 'a mandatory data retention regime raises fundamental

---

[157] Ibid Terms of Reference.
[158] Ibid vol 3, 2484.
[159] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2007 (Cth) 6.
[160] Australian Law Reform Commission, above n 153, vol 3, 2485.
[161] Ibid.
[162] 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) 1.
[163] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, Discussion Paper (July 2012) 7-8.
[164] Ibid 10.
[165] Parliamentary Joint Committee on Intelligence and Security, above n 159, 6 [1.31].
[166] Ibid 6 [1.30].

privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed'.[167]

The Discussion Paper prepared by the Attorney-General's Department that was aimed at informing the 2013 PJCIS Inquiry and accompanies the report, notes that the reason why mandated metadata retention is necessary is because service providers are progressively limiting the metadata that they retain for business purposes and thus that data is no longer available for law enforcement and national security agencies ('**LENS Agencies**') to use in their investigations.[168] The reason why metadata is used by LENS Agencies is that it is a 'cost-effective investigative [tool] that supports and complements information derived from other sources'.[169] Moreover, '[metadata] is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest'.[170]

Submissions made to the 2013 PJCIS Inquiry expressing concern regarding the implementation of a metadata retention regime came from individuals in their private capacity and non-governmental organisations, focusing chiefly on impacts upon privacy and harms arising from privacy intrusion. Both the Law Council of Australia and the Institute of Public Affairs expressed their concerns stating that such a proposal is neither necessary nor proportionate to the threat faced by Australia from serious criminal activity or national security threats,[171] and that any such regime would 'render any presumed or existent Australian right to privacy empty'.[172]

The Inquiry was told that through the use of mandatory metadata retention, the government shifted its perception of society from being generally innocent, to requiring constant surveillance – with the presumption that all persons are potential criminals.[173] The Australian Interactive Media Industry Association's Digital Policy Group noted in a similar vein that a mandatory metadata retention regime '[raises]...concerns about the presumption of guilt' of the individual, reversing the presumption of innocence.[174] This position was echoed by the Victorian Privacy Commissioner, noting that mandatory metadata retention was 'characteristic of a police state' and contrary to 'essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusion into a person's life'.[175] The Inquiry was further told that the collection of personal information in the form of metadata in and of itself amounted to unjustified privacy intrusion. Liberty Victoria noted that a move

[167] Ibid 7 [1.35].
[168] Attorney-General's Department, above n 160, 21.
[169] Ibid 14.
[170] Ibid 21.
[171] Parliamentary Joint Committee on Intelligence and Security, above n 159, 150 [5.41].
[172] Ibid 150 [5.42].
[173] Ibid 150-151 [5.45].
[174] Ibid 152 [5.52].
[175] Ibid 153 [5.55].

away from the targeted interception to metadata retention 'constitutes a significant intrusion into the privacy of each end user of telecommunications service and creates a situation in which a single security breach would have dramatic consequences'.[176] Liberty Victoria submitted that the very fact of the existence of this trove of data will encourage future extensions to the purposes for which it may be used.[177] This 'mission creep' is already being witnessed and will be discussed in greater detail later in this section.

The Inquiry heard that in order for privacy to be adequately protected in the digital age, policies of data minimisation should be implemented - '[where] there is no personal information, there is no consequent duty of care' to ensure the protection of personal information against unauthorised or secondary use.[178] This problem is highlighted by the submission made by Electronic Frontiers Australia, which noted that it is increasingly difficult to distinguish between metadata and content of communication. The concern is that the examination of metadata 'will reveal highly intimate details of a person's life including 'religious and political affiliations, sexual orientation, health issues and other highly-sensitive information'.[179] For instance, with respect to internet browsing, the Inquiry heard that it would be next to impossible to separate metadata from content due to the fact that structure of websites, the 'back-end' programming that comprises the bulk of the metadata, often includes sensitive information that is by definition content – such as usernames, passwords, and key words.[180] Fundamentally, the difficulty in accepting the metadata retention regime lies in its potential for privacy violations by future governments through 'mission-creep', *ultra vires* access to data by authorised entities, and unauthorised access by third parties and data breaches.[181] As suggested by the United Nation's Special Rapporteur, this would require a comprehensive, transparent and independent oversight mechanism in place to ensure appropriate use of stored metadata.[182]

Conversely, the LENS Agencies have put forward submissions making the point that, in the digital era, the retention of metadata was a necessary process to ensure the continued effectiveness of organisations tasked to protect society against serious criminal and national security threats.[183] As telecommunication service providers are limiting the amount and the time frame they retain metadata, mandatory retention is necessary for the protection of society.[184] Moreover, the LENS Agencies assured the Inquiry that the retention of metadata does not represent 'an expansion of their power, and thus does not translate into any serious diminution of privacy or a winding back of civil

[176] Ibid 151-152 [5.49].
[177] Ibid 152 [5.50].
[178] Ibid 151 [5.47].
[179] Ibid 156 [5.69]-[5.70].
[180] Ibid 157 [5.73]-[5.74].
[181] Ibid 158 [5.77].
[182] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda item 3, UN Doc AHRC/17/27 (16 May 2011) 10 [32].
[183] Parliamentary Joint Committee on Intelligence and Security, above n 159, 161-162 [5.95], [5.98].
[184] Ibid 162-3 [5.98]-[5.99].

liberties'.[185] This claim was made in light of the fact that the LENS Agencies could, under certain circumstances, request metadata without a warrant.[186] Further, the LENS Agencies note that apart from being a necessary tool, metadata represents a lesser intrusion into privacy 'as it relates to [metadata] rather than its content, it raises fewer privacy concerns than the other covert investigative methods'.[187] The data is stored and controlled by the telecommunication service providers themselves and only accessed when properly authorised, 'as such, mandating [metadata] retention will not lead to the removal of the presumption of innocence [and metadata] will continue to be accessed only in connection with active investigations'.[188]

With regard to the submissions made concerning the difficulty of separating content from metadata, the LENS Agencies recognised the potentialities of content being disclosed and noted that the 'TIA Act does not permit the disclosure of the content or substance of a communication without a warrant'.[189] Furthermore, the Australian Federal Police, Australian Security and Intelligence Organisation and the Australian Crime Commission, in a joint submission stated that they 'do not want the internet browsing history of every customer of an [internet service provider] to be retained'.[190] The submission from the Attorney-General's Department stated that there were sufficient safeguards to separate metadata from content, that the LENS Agency 'has to [be satisfied] internally that they are seeking information that would fall within a definition of [metadata]...The final decision is with the industry player, and if they cannot extrapolate data from content, then they cannot disclose that'.[191]

Having considered the submissions made, the Committee for the 2013 PJCIS Inquiry made a number of comments and two recommendations regarding the mandatory retention of metadata. Firstly, the Committee pointed out that the proposal to retain metadata lacked any draft legislation so the consultation process could only be rather general. However, in noting this, the Committee also stated that the difficulty in implementing such a regime would come from the balancing of competing interests of protecting national security and protecting the privacy of individuals within a significantly altered relationship between the state and the person. The Committee stated that 'no such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed'.[192] The following recommendations were made as the result of this Inquiry:

1. Any metadata retention regime should explicitly exclude content data;
2. Internet browsing data should be explicitly excluded;

[185] Ibid 161 [5.92].
[186] Ibid 161[5.93].
[187] Ibid 161-2 [5.95]-[5.96].
[188] Ibid 161 [5.94].
[189] Ibid 164 [5.105].
[190] Ibid 164 [5.104].
[191] Ibid 164 [5.107].
[192] Ibid 190 [5.206]-[5.208].

3. Where metadata cannot be separated from content, this should be treated explicitly as content and require a warrant for lawful access;
4. Metadata retained under this regime should be encrypted for secure storage; and
5. An independent audit scheme should be established.[193]

C Metadata Retention Legislation

The Telecommunications (Interception and Access) (Data Retention) Bill 2014 (Cth) ('**the Bill**') was introduced into the Australian Federal Parliament on 30 October 2014. It was a Bill intended to amend, amongst others, the TIA Act, the Telecommunications Act, and the Privacy Act to 'require companies providing telecommunications services in Australia, carriers and internet service providers to keep a limited, prescribed set of [metadata information] for two years'.[194] The amending legislation passed both houses of Parliament in April 2015.

As neither the Bill nor the TIA Act contain a Long Title, a Preamble or an Objects clause, it is necessary to refer to extrinsic sources to ascertain the Parliamentary intention behind the Bill. Malcolm Turnbull, then-Minister for Communication responsible for introducing the Bill to Parliament, justified this legislation based on the positions of LENS Agencies stating that '[m]odern communication technologies have revolutionised the abilities of people to communicate, collaborate, and express themselves...these same technologies are routinely misused and exploited by criminals, including those who threaten our national security'.[195] In his second reading speech, Mr Turnbull argued that access to historical metadata was necessary as it is used in 'almost every counter-terrorism, counter-espionage, cyber security and organised crime investigation. It is also used in almost all serious criminal investigations including...murder, serious sexual assaults, drug trafficking and kidnapping'.[196] Finally, the extended nature of investigations, often spanning years, justified the retention of historical metadata for a period of two years.[197]

Thus, the amendment requires telecommunications service providers to retain subscribers' and users' metadata for a period of two years.[198] In section 187AA, the TIA Act prescribes the 'kinds of information' that a service provider must keep, indicating that the list provided is not an exclusive list of information to be retained. The categories of data to be retained includes:

1. The subscriber, account, telecommunications devices and services available on the account;
2. The source of the communication;
3. The destination of the communication;

---

[193] Ibid 190-193.
[194] Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12562 (Malcolm Turnbull, Minister for Communication).
[195] Ibid 12560.
[196] Ibid.
[197] Ibid 12561.
[198] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187C.

4. The date, time and duration of the communication;
5. The type of communication utilised; and
6. The geolocation of the line, equipment or telecommunications device.[199]

Under the amendment to the TIA Act, the information thus retained is to be considered 'personal information' for the purposes of the Privacy Act.[200] Part of the parliamentary intention in passing this legislation was to limit the number of government (and non-governmental) agencies who could previously request access to an individual's metadata without a warrant. Prior to the amendments enshrined in the TIA Act, over 80 organisations sought and obtained access to individual's metadata and no warrant was required for such access;[201] according to the Federal Attorney-General George Brandis, following the amendment, the number of agencies that would have access to metadata without a warrant would be limited to 21.[202] Curiously, when examining the TIA Act, only 14 state and Federal agencies have been explicitly granted access to metadata under the TIA Act; it is unclear what the remaining seven agencies are referred to by the Attorney-General.[203] The TIA Act provides that the minister may, by legislative instrument, declare any other organisation to be a 'criminal law-enforcement agency' within the meaning of the Act.[204] Other changes implemented with the enactment of the Bill are the establishment of the Journalist Information Warrant regime and a statutory position of a Public Interest Advocate.

1 *Journalist Information Warrant and the Public Interest Advocate*

In the first iteration of the Bill, access to journalists' metadata was also allowable without warrant. In the six months of parliamentary debate surrounding this amendment, concern raised by parliamentarians, legal and rights groups, and members of the public caused a scheme to be included in the legislation whereby the LENS Agencies would be required to seek a warrant to access a journalists' metadata. The 2015 Parliamentary Joint Committee on Intelligence and Security ('**2015 PJCIS Inquiry**') heard that a journalist's source could be easily identified with the use of this retained

[199] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of Legislation in Accordance with the Human Rights (Parliamentary Scrutiny) Act 2011*, 15th Report, 44th Parliament (November 2014) 11; *Telecommunications (Interception and Access) Act 1979* (Cth) s 187A(2). The legislated list that is found in section 187AA of the TIA Act illustrated the information to be retained by the telecommunications service is extracted and annexed hereto as Annexure B.
[200] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187LA.
[201] Stephanie Anderson, 'List of agencies applying for metadata access without warrant released by Government', *ABC News* (online), 18 January 2016 <http://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836>. The full list of agencies and organisation is found at this link: https://www.documentcloud.org/documents/2693008-List-of-Agencies-That-Applied-for-Metadata.html.
[202] Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2245 (George Brandis, Attorney-General).
[203] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5, 110A, 176A.
[204] Ibid s 110A(3).

data.[205] The Australian Media, Entertainment & Arts Alliance specifically noted that easy access to the journalists' metadata would have a 'chilling effect on any potential whistleblower or confidential source releasing information [the Government] would not want to release'.[206] This was supported by the Law Council of Australia in their submission, stating that 'significant risks [of metadata retention] include attempting to determine journalists' sources'.[207] Following a ranges of submissions, the Inquiry commented that in the context of journalists and their sources, there is potential for a chilling effect on disclosure of information.[208] A follow up inquiry specifically convened for the purpose of examining the question of metadata being used to identify a journalists' source made the following two recommendations:

1. The introduction of a journalist information warrant regime; and
2. Establishment of a Public Interest Advocate.[209]

In subsequent Parliamentary debates, Jacinta Collins MP stated that 'there will be a statutory presumption against issuing the warrant and agencies will be required to prove that the public interest in obtaining the metadata outweighs the public interest in protecting the confidentiality of a journalist's source'.[210]

As passed, the legislation follows two distinct yet similar processes for obtaining a journalist information warrant – one for the Australian Security and Intelligence Organisation ('**ASIO**') (referred to in the TIA Act as 'the Organisation') and one for the remaining 13 (or 20) agencies specified under the TIA Act. With respect to ASIO, the Director-General of Security may request the Minister to issue a journalist information warrant under section 180J.[211] Authorisation for a journalist information warrant for the remaining agencies is made by an 'authorised officer'[212] of the organisation applying to an 'issuing authority'[213] within the meaning of the TIA Act under section 180Q.[214]

The relevant test for all requests for a journalist information warrant is if the Minister or the issuing authority is satisfied that 'the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the…source',[215] based on the following considerations:

---

[205] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (February 2015) 63 [2.187].
[206] Ibid 64-5 [2.192].
[207] Ibid 221 [6.108].
[208] Ibid 257 [6.124]
[209] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source* (March 2015) 1-2.
[210] Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2126 (Jacinta Collins).
[211] *Telecommunications (Interception and Access) Act 1979* (Cth) s 180J.
[212] Ibid s 5(1).
[213] Ibid s 6DB.
[214] Ibid s 180Q.
[215] Ibid ss 180L(2)(b), 180T(2)(b).

1. The extent to which the privacy of any person or persons would be likely to be interfered with;
2. The gravity of the matter in relation to which the warrant is sought;
3. The extent to which that information or those documents would be likely to assist in the performance of the functions of the enforcement agencies;
4. Whether reasonable attempts have been made to obtain the information or documents by other means;
5. Any submissions made by the Public Interest Advocate; and
6. Any other matter that the Minister or the issuing authority considers relevant.[216]

The TIA Act allows for a Public Interest Advocate to make submissions to a closed court on the public interest of issuing the journalist information warrant.[217] However, problems with this system have been identified: firstly, the affected journalist will not be privy to the fact that their metadata is being sought, and disclosure of this fact (or that the warrant has been issued) is punishable by 2 years' imprisonment;[218] secondly, the authorities requesting the warrant have the resources and time to properly prepare their application for the warrant - they are unconstrained in preparing their application. Conversely, the Public Interest Advocate must respond to the application by preparing submissions within seven days.[219] Thirdly, there will not exist a database of past warrant applications and the determinations thereof for the Public Interest Advocate to use for reference; and lastly, there does not appear in the TIA Act or explanatory documentation any provision for the Public Interest Advocate to be able to call witnesses or be allowed time to prepare adequate evidence (beyond the seven days mentioned).[220]

2 Additional Impacts of the TIA Act Amendments

One of the seemingly unintended consequences of the amendment deals with the interaction of sections 178, 179 and 180 of the TIA Act. These sections deal with access to metadata under particular circumstances – section 178 applies to retained data for the purpose of the enforcement of criminal law, stating that an 'authorised officer must not make the authorisation unless [they are] satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law';[221] section 179 applies to retained data to be used for enforcement of a law imposing a pecuniary penalty or for the protection of public revenue, stating that an 'authorised officer must not make the authorisation unless [they are] satisfied that the disclosure is reasonably necessary for the

[216] Ibid.
[217] Ibid s 180X.
[218] Ibid s 182A(1).
[219] *Telecommunications (Interception and Access) Regulations 1987* (Cth) reg 9.
[220] Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2242-2243 (Nick Xenophon).
[221] *Telecommunications (Interception and Access) Act 1979* (Cth) s 178(3).

enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue'.[222] However, section 180 allows access to metadata prospectively, with the following wording: an 'authorised officer must not make the authorisation unless [they are] satisfied that the disclosure is reasonably necessary for the investigation of: a) a serious offence;[223] or an offence against the law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years'.[224]

Sections 171 to 180 (with the exception of sections 176A and 178A) were inserted into the legislation in 2007 by the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth), allowing for advances in technology to facilitate law enforcement purposes. The 2007 amendments to the TIA Act did not allow for the bulk collection and retention of metadata – telecommunication service providers did not have standardised retention procedures so the value of retained data was less than what could have been required to be retained under a section 180 prospective order. However, with the addition of the standardised metadata retention for the period of two years, the value of the more stringent test to acquire prospective metadata is effectively bypassed. The practical impact of this reading of the relevant sections is that metadata can be used to investigate any form of criminal behaviour, no matter how minor. This will be discussed in greater detail shortly.

Additionally, besides the issues discussed above relating to the journalist information warrant and the Public Interest Advocate, it appears that the manner in which the journalist information warrant is obtained lacks procedural fairness, regardless of whether the warrant is obtained through sections 180J or 180Q of the TIA Act. Section 182A of the TIA Act specifies that disclosure to any person of whether a journalist information warrant is being requested, has previously been requested, has been granted, or has been revoked is punishable by 2 years' imprisonment. With respect to a journalist information warrant issued to ASIO, the only persons entitled to know of the issuing of the warrant are the Minister[225] and the Director-General of Security.[226] The Director-General must then notify the Inspector-General of Security who, in turn, notifies the Minister;[227] the Minister must then notify the PJCIS.[228] Each of these processes of notification takes place 'as soon as practicable', with little guidance as to what that entails. A journalist information warrant granted to the AFP, the Minister and the Commonwealth Ombudsman must be notified and the Minister must notify the PJCIS;[229] alternatively, for every other authorised agency, the chief officer of that agency must notify the

[222] Ibid s 179(3)
[223] As defined in the *Telecommunications (Interception and Access) Act 1979* (Cth) s 5D, meaning an offence of the type of murder, kidnapping, terrorism or one that punishable by at least 7 years' imprisonment; this is not an exhaustive list of offences constituting a 'serious offence' under the TIA Act.
[224] *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(4).
[225] Ibid s 185D(1)(b).
[226] Ibid s 185D(1)(a).
[227] Ibid s 185D(3).
[228] Ibid s 185D.
[229] Ibid s 185D(5)(a).

Commonwealth Ombudsman.[230] Again, this process of notification takes place 'as soon as practicable'. Lastly, the Commonwealth Ombudsman must inspect the records of the LENS Agencies[231] and prepare a report to the Minister once per financial year,[232] which must be tabled before each House of Parliament within 15 sitting days of that House after the Minister receives the report.[233]

This leads to a situation where at no point is the person subject of a warrant ever notified of the existence of that warrant and consequently is unable to challenge or dispute the administrative decisions made regarding their personal information. The case of *Kioa v West* applies to the administrative decision-making 'which affects rights, interests and legitimate expectations, subject only to the clear manifestation of a contrary statutory intention'.[234] Though the notion of legitimate expectation is questionable under Australian law, the concept of procedural fairness is well-established in terms of the exercise of statutory power.[235] And yet, the process of obtaining of the journalist information warrant is highly opaque, with oversight initially undertaken by the very entity authorising disclosure and by an independent body only at a time thereafter. This does not accord with the requirements of procedural fairness, whereby 'statutory power...must be exercised in accordance with procedures that are fair to the individual considered in light of the statutory requirements'.[236] This is particularly the case with respect to the average individual who does not have the benefit of a Public Interest Advocate to review the application for access to their metadata.

D *Parliamentary Inquiries into the Amendment of the TIA Act*

Prior to the Bill being passed, it was discussed as part of a number of Parliamentary inquiries, chiefly – the 2014 Parliamentary Joint Committee on Human Rights ('**2014 PJCHR Report**') and the 2015 PJCIS Inquiry. The 2015 PJCIS Inquiry recalled the efforts of the earlier, 2013 PJCIS Inquiry and noted that not all recommendations made by the previous committee have found their way into the Bill; the Committee for the 2015 PJCIS Inquiry urged the Government to respond to all of the previous recommendations but stated that that should not delay the debate of the Bill.[237] The 2015 PJCIS Inquiry is informed by the Bill that was prepared on the recommendation of the 2013 PJCIS Inquiry, the submissions made to the 2015 Inquiry and the three versions of the Explanatory Memoranda prepared relating to the Bill.

---

[230] Ibid s 185D(5)(b).
[231] Ibid s 186B(1).
[232] Ibid s 186J.
[233] Ibid s 186J(3).
[234] *Kioa v West* (1985) 159 CLR 550, 584.
[235] Matthew Groves, 'Substantive legitimate Expectations in Australian Administrative Law' (2008) 32 *Melbourne University Law Review* 470, 471.
[236] *Kioa v West* (1985) 159 CLR 550, 585 (Mason J).
[237] Parliamentary Joint Committee on Intelligence and Security, above n 202, 1-2.

1 *International Standard of Privacy Protection*

The 2014 PJCHR Report contained an examination of the requirements for lawful infringement of an international legal right to privacy based on article 17 of the ICCPR, stating that 'permissible limitations...are provided by law and are not arbitrary. For limitations not to be arbitrary, they must seek to achieve a legitimate objective and be reasonable, necessary and proportionate to achieving that objective'.[238] Indeed, the 2015 PJCIS Inquiry noted that the Attorney-General's Department gave evidence before the Senate Standing Committee on Legal and Constitutional Affairs ('**SSCLCA**'), which was holding hearings at around the same time. The Attorney-General's Department gave evidence that:

> Article 17 of the International Covenant on Civil and Political Rights sets out the right of the persons to be protected against arbitrary or unlawful interference with their privacy. In order to avoid being arbitrary, any interference with privacy must be *necessary* to achieve the *legitimate purpose* and *proportionate* to that purpose.[239] [Emphasis added]

Timothy Pilgrim, the-then Australian Privacy Commissioner, referred to the test for allowable privacy intrusion put forward by the Office of the United Nations High Commissioner for Human Rights:

> The limitation must be *necessary* for reaching *a legitimate aim*, as well as *in proportion to the aim and the least intrusive option available*. Moreover, the limitation placed on a right (an interference with privacy, for example, for the purpose of protecting national security or the right to life of others) must be shown to *have some chance of achieving that goal*.[240] [Emphasis added]

Furthermore, both the 2014 PJCHR Report and the 2015 PJCIS Inqury referred to the principles and reasoning laid out in the European Court of Justice decision in the *Digital Rights Ireland Case*, which examined the legality of metadata retention under the law of the European Union.[241] As previously noted, the *Digital Rights Ireland Case* involved the European Union seeking to implement the Directive 2006/24/EC ('**the Directive**') requiring member states to collect and retain personal metadata of telecommunication users in Europe for the purposes of aiding criminal and national security investigations. Importantly, the Directive, including the data set to be retained, formed the model for Australia's metadata retention legislation.[242] The European Court's reasoning in determining the *Digital Rights Ireland Case* closely followed the tests elaborated above, reviewing the

---

[238] Parliamentary Joint Committee on Human Rights, above n 196, 11 [1.25].
[239] Parliamentary Joint Committee on Intelligence and Security, above n 202, 36 [2.97].
[240] Ibid 36-37 [2.98]; Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) [23].
[241] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (C-293/12) [2014] ECJ 238, [27] ('*Digital Rights Ireland Case'*).
[242] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (February 2015) Appendix A; the Federal Attorney-General's Department who prepared the data set, in Appendix A noted that '[t]he categories of data are closely based on the European Union Data Retention Directive'.

matter in dispute in light of consideration of whether the law was necessary and effective,[243] and proportionate to achieve a legitimate aim.[244] While the decision of the Court in the *Digital Rights Ireland Case* is not binding in Australia, the similarity of the legislative provisions and the tests of legality applied by the Court mean that the decision can be seen as influential. This is especially so since the decision of the Court mirrors the best-practice approach to privacy protection articulated by the United Nations Human Rights Council.[245] As such, the consideration of effectiveness, necessity, and proportionality is the test that will be applied presently and will form the basis of analysis regarding whether the metadata retention regime breaches the requirement of the protection the individual right to privacy found in article 17 of the ICCPR.

(a) Is Metadata Retention Effective?

The 2015 PJCIS Inquiry considered whether metadata retention is effective to achieve a legitimate aim. To be considered effective, metadata retention must be shown to have 'some chance of achieving' the stated goal.[246] With regard to the effectiveness of metadata retention, the Inquiry heard submissions that circumvention of the regime would be a simple matter of the use of Virtual Private Networks and other modern technologies.[247] Conversely, the Inquiry heard that while some criminal elements may adopt new technologies to avoid detection of their online activities by way of retained metadata, the majority of criminals are not adapt at implementing technological counter-strategies.[248] Thus, the argument presented by proponents of a metadata retention regime suggests that investigators should have access to investigatory tools regardless of whether some potential surveillance targets would implement counter-surveillance strategies.[249] The LENS Agencies submitted that the ability to retain metadata is vital to ensure the efficacy of complex investigations into 'counter-terrorism, child protection and organised crime'.[250] The Inquiry further noted the impact of a similar metadata retention scheme implemented in the European Union;[251] having reviewed a European Commission's *Evaluation Report*, the Inquiry quoted from the Report saying that people did not change their communications behaviour in response to metadata retention regimes, contrary to fears put forward by civil society groups. With regard to the impact on individual communications behaviour, the Report was quoted as saying that 'there is no corroboratory evidence for any change

---

[243] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [41], [43]-[44].
[244] Ibid [47]-[49], [54]-[69].
[245] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014).
[246] Parliamentary Joint Committee on Intelligence and Security, above n 202, 46 [2.129].
[247] Ibid 46 [2.130]-[2.131].
[248] Ibid 47-8 [2.134]-[2.135].
[249] Ibid 47 [2.133].
[250] Ibid 47 [2.132]-[2.134].
[251] *Directive 2006/24/EC/ of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54.

in behaviour having taken place in any Member State concerned or in the EU generally'.[252] With respect to the *Evaluation Report*, the 2015 PJCIS Inquiry appears to be referencing the fear that even the potential ubiquitous surveillance would encourage individuals to monitor and censor their communications (as previously discussed); however, the portion of the report being quoted refers specifically to the financial cost associated with the implementation of metadata retention scheme and the financial burden of the scheme being passed on to the consumer. The same paragraph of the Report notes that '[t]here is no evidence of any quantifiable or substantial effect of the [metadata retention] Directive on consumer prices for electronic communications services'.[253] In referring to the above quote devoid of context, the 2015 PJCIS Inquiry appear to have fallen into error, either by misunderstanding the meaning and context of the EU Report or by seeking to misrepresent the Report's conclusions.

Further to the matter of effectiveness of the legislation, an additional difficulty arises when considering that the law that was aimed at limiting the number of agencies that previously had access to retained metadata is reportedly failing at this task. On at least two occasions, the Federal Attorney-General's department were made aware that entities not specifically authorised under the TIA Act were gaining access to retained metadata by other means. In their justification for the passing of the metadata retention amendments to the TIA Act, the Government asserted that these changes will limit the number of agencies able to access retained metadata to 21 agencies provided in the legislation, with additional agencies to be added by an act of Parliament.[254] As discussed, the number of prescribed agencies listed in the legislation is 14 and it is uncertain when considering the legislation to which other agencies the Attorney-General was referring. Nonetheless, this represents a significantly lesser number of agencies that were able to access metadata prior to the amendment.[255] This limitation however, has not prevented Federal Government departments from seeking access to metadata by applying to the AFP to conduct the searches for them.[256] In that report, the spokesperson for the Department of Social Services is quoted as saying '[a]dvice was provided by the Attorney-General's Department to [the Department of Social Services] that any organisation not listed in the legislation may wish to engage with law enforcement about being able to access [metadata] for criminal investigative purposes'.[257] This statement was followed by one from a spokesperson from the Federal Attorney-General's Department, commenting that access to metadata may only be

[252] Ibid 49 [2.138].
[253] European Commission*, Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* [2011] 26.
[254] Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2245 (George Brandis, Attorney-General).
[255] This is a list of agencies that had access to individual's metadata prior to the amendment of the TIA Act: <https://www.documentcloud.org/documents/2693008-List-of-Agencies-That-Applied-for-Metadata.html>.
[256] Benjamin Sveen, 'Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted', *ABC News* (online), 04 October 2016 <http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648>.
[257] Ibid.

authorised for investigative purposes where reasonably necessary to enforce criminal law and that '[i]f departments without access believe the law has been breached, they can alert law enforcement agencies'.[258]

Moreover, it appears that aside from the advice of the Attorney-General's Department, other organisations that were intended by Parliament to lose access to retained metadata are finding other means of accessing the information by way of section 280 of the *Telecommunications Act 1997* (Cth). Section 280 allows for any organisation or agency to obtain disclosure that is authorised by or under law.[259] Agencies excluded from obtaining metadata information under the amendments to the TIA Act have been circumventing the intent of Parliament by relying on other relevant legislation to justify access under section 280. First raised as an issue in 2015, Leonard noted that numerous agencies that have not been expressly authorised under the TIA Act to access retained metadata, would still have access pursuant to this provision.[260] This issue was brought to light again by the Communications Alliance in their submission to the Federal Attorney-General's Department inquiry into *Access to Telecommunications Data in Civil Proceedings*.[261] The Communications Alliance asserted that organisations as diverse as local councils, the RSPCA, and the Environmental Protection Authority are using the section 280 powers in order to obtain metadata, access to which would otherwise be forbidden under the TIA Act (unless an authorised organisation could be convinced to obtain access). Crucially, disclosure under section 280 of the *Telecommunications Act 1997* (Cth) does not require the appointment of a Public Interest Advocate (if the metadata pertains to a journalist) as would be required under section 180X of the TIA Act; the person entrusted with the decision to disclose retained metadata does not need to be satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law pursuant to section 178(3) of the TIA Act; nor must the person entrusted with the decision to disclose retained metadata consider privacy pursuant to section 180F of the TIA Act.[262]

It is of concern that the Government department charged with 'maintaining and improving Australia's law and justice framework'[263] appears to be encouraging agencies to work around the safeguards limiting access to retained metadata to specific agencies for specific purposes. As noted, one of the stated intentions of Parliament in passing the metadata amendments to the TIA Act was to limit the range of organisations and agencies that would have access to individual metadata. Thus, having

[258] Ibid.
[259] *Telecommunications Act 1997* (Cth) s 280(1)(b).
[260] Peter Leonard, 'Mandatory internet data retention in Australia: Looking the horse in the mouth after it has bolted' (2015) 101 *Journal of the Intellectual Property Society of Australia and New Zealand* 43, 56.
[261] Communications Alliance, Submission to the Attorney-General's Department, Parliament of Australia, *Access to Telecommunications Data in Civil Proceedings*, 27 January 2017, 5.
[262] Ibid.
[263] Attorney-General's Department, Parliament of Australia, *About Us* <https://www.ag.gov.au/About/Pages/default.aspx>.

unauthorised entities access retained metadata through circuitous means shows that the legislative amendment is of limited effectiveness. As such, it appears that the metadata retention regime lacks the requirement of effectiveness to be considered valid under article 17 of the ICCPR.

(b) Is Metadata Retention Necessary?

To be considered necessary, the aim of the legislation must be necessary in the circumstances.[264] The Replacement Explanatory Memorandum notes that the legitimate aims of the metadata retention regime are 'the protection of national security, public safety, addressing crime, and protecting the rights and freedoms of individuals [achieved by way of the] retention of a basic set of communications data required to support relevant investigations'.[265] In support of the necessity of mandatory metadata retention, the 2014 PJCHR concluded that 'the statement of compatibility has generally established why particular categories of data are considered necessary for law enforcement agencies'.[266] However, the Law Council of Australia, Law Institute of Victoria, the various Councils for Civil Liberties throughout Australia, as well as the United States' Privacy and Civil Liberties Oversight Board, submitted that there is little evidence in support of the efficacy and usefulness of metadata retention in the prevention of terrorist attacks or combating serious crime.[267] Moreover, one study commissioned by the German Ministry of Justice showed that between 2008 and 2010 when both Germany and Switzerland trialled metadata retention, there was no measurable effect on crime clearance rates.[268] The various councils for civil liberties in their joint submission, accepted that metadata may be an important investigative tool. However, they also expressed concern and scepticism regarding the 'mass collection and retention of [metadata] of non-suspect citizens for retrospective access' and the argument that this retained data will aid the LENS Agencies in combating terrorism and serious crime.[269]

Nonetheless, the 2015 PJCIS Inquiry, like the earlier inquiry of 2013, heard that the utility of retained metadata lies in the fact that metadata 'is critical to the investigation of almost any criminal activity, serious or otherwise'.[270] The 2015 Inquiry heard from the LENS Agencies that metadata 'is used extensively, and provides significant value, in serious and complex investigations'.[271] The Committee

---

[264] Niloufer Selvadurai, 'The Retention of Telecommunications Metadata: A Necessary National Security Initiative or a Disproportionate Interference with Personal Privacy?' (2017) 23(2) *Computer and Telecommunications Law Review* 35, 38.
[265] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 12.
[266] Parliamentary Joint Committee on Human Rights, above n 196, 12 [1.30].
[267] Parliamentary Joint Committee on Intelligence and Security, above n 202, 38-40 [2.106]-[2.111].
[268] Ibid 39-40 [2.108], [2.110]. The German experience found that in the two years between 01 January 2008 and 02 March 2010, crime clearance rates were reduced by a mere 0.006%: German Working Group on Data Retention (AK Vorrat), *Criminologists: No "security gap' without blanket communications data retention* (08 February 2012) <http://www.vorratsdatenspeicherung.de/content/view/534/55/lang,en/>.
[269] Parliamentary Joint Committee on Intelligence and Security, above n 202, 39 [2.109].
[270] Ibid 16 [2.28].
[271] Ibid 16 [2.29].

further reviewed classified evidence from the-then Acting Director-General of Security and ASIO regarding the use and utility of metadata in terrorism investigations, which stated that 'had relevant [metadata] not been available to ASIO [it] would have been blind to critical information, including the existence of covert communications between members of terrorist groups' in relation to particular investigations.[272] Apart from terrorism and counterespionage operations,[273] the 2015 Inquiry was told that the Australian Federal Police ('**AFP**') use metadata to:

> [I]dentify suspects and/or victims, exculpate uninvolved persons, resolve life threatening situations like child abductions or exploitation, identify associations between members of criminal organisations, provide insight into criminal syndicates and terrorist networks, and establish leads to target further investigative resources.[274]

Further, the Attorney-General's Department drew the Inquiry's attention to the 2006 European Commission report that recommended the institution of a metadata retention regime in the European Union ('**EU**'), stating that regardless of the limited evidence of efficacy, metadata retention plays an important role in criminal investigations, and that the use of metadata has resulted in 'convictions for criminal offences which, without [metadata retention], might never have been solved. It also resulted in acquittals of innocent persons'.[275] The proponents of the metadata retention regime argued that retention of metadata was imperative, amongst other reasons, for the protection of human rights; specifically for the prosecution of persons guilty of committing crimes against the individual and the state, as well as ensuring that persons who are innocent are not falsely convicted.[276] This argument was put to the SSCLCA where the Attorney-General noted that the LENS Agencies have an obligation to protect an individual's right to physical safety and the right to life, and that metadata retention is necessary to 'investigating past crimes and deterring and preventing future crimes'.[277] Mention was made of a draft Resolution of the United Nations Human Rights Council of 2008 calling on all governments:

> To establish mechanisms, where appropriate, in cooperation with the international community, to combat the use of the Internet to facilitate trafficking in persons and crimes related to sexual or other forms of exploitation and to strengthen international cooperation to investigate and prosecute trafficking facilitated by the use of the Internet.[278]

On the other hand, the LENS Agencies submitted that, while there is a need for access to metadata in furthering intelligence and criminal investigations, the use and access to this data is limited; ASIO

---

[272] Ibid 16-7 [2.30].
[273] Ibid 17 [2.31]-[2.32].
[274] Ibid [2.33].
[275] Ibid 40 [2.112].
[276] Ibid 44-46 [2.123]-[2.128].
[277] Ibid 44 [2.124].
[278] Ibid 44-5 [2.125]; Human Rights Council, *Special Rapporteur on Trafficking in Persons, Especially Women and Children*, 8th sess, UN Doc A/HRC/8/L.17 (12 June 2008) [2(g)]. This draft Resolution was eventually passed: Human Rights Council, *Special Rapporteur on Trafficking in Persons, Especially Women and Children*, 8th sess, UN Doc A/HRC/RES/8/12 (18 June 2008) [2(g)].

advised the Inquiry that it does not engage in 'large-scale mass gathering of communications data' and that it 'does not have the resources, the need, or the inclination' to undertake such mass intelligence gathering. Nevertheless, this is precisely what the amendments to the TIA Act require telecommunications service providers to do. In its submission, ASIO asserted that at most, a few thousand people per year come to ASIO's attention requiring access to their telecommunications data.[279] This was added to by the Inspector-General of Intelligence and Security, who submitted that any ASIO 'inquiries and investigations into individuals and groups must be undertaken using as little intrusion into individual privacy as possible'.[280] These assertions from Government put to question the veracity of the assertion of the need to retain metadata. Indeed, the Law Council of Australia noted in their submission that the LENS Agencies have not articulated a deficiency in the regime existing prior to the implementation of metadata retention to demonstrate a gap in capability.[281] Given that metadata was accessed prior to the implementation of the amendments, it was not clearly articulated or empirically demonstrated by the LENS Agencies how mandatory retention would aid their investigatory capabilities. Indeed, studies that have been conducted show a limited usefulness, however it should be noted that there was a lack of consistency in the data retained by the various telecommunications service providers prior to the implementation of the metadata retention regime.[282]

Finally, the LENS Agencies submitted to the 2015 PJCIS Inquiry that there are strict limitations on their access to historical metadata; South Australia Police noted that reasonable necessity and relevance are core elements of the statutory test to access historical metadata.[283] However, as was discussed in an earlier section, this still represents a test that is significantly lower than that applied to metadata to be retained prospectively. The end result is that, while the LENS Agencies (with the exception of ASIO) must prove reasonable necessity, there is no requirement that the metadata be used for the investigation of crimes of a serious nature. This, as has been suggested by the Court in *Digital Rights Ireland Case*, leads to the situation where the seriousness of the interference with the right to individual privacy is disproportionate to the actual object pursued by the interference.[284]

The Attorney-General's Department submitted that due to the declining ability of the LENS Agencies to reliably access the *content* of communications due to technological change, it was therefore necessary for metadata to be reliably available for investigative purposes.[285] However, due to

[279] Parliamentary Joint Committee on Intelligence and Security, above n 202, 53-4 [2.155].
[280] Ibid 54 [2.156].
[281] Ibid 24 [2.55].
[282] Ibid 60 [2.179].
[283] Ibid 20 [2.42].
[284] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [47].
[285] Parliamentary Joint Committee on Intelligence and Security, above n 202, 26 [2.60]-[2.62]; moreover, while content requires a prospective warrant to be accessed, historical metadata is accessed more easily requiring simply an authorisation from an authorised officer within one of the LENS Agencies.

changing nature of the telecommunications and internet service provider's billing practices, metadata was not as readily retained.[286] Thus, the retention of metadata on a mandated basis is required for criminal investigatory and national security purposes. However, the Inquiry noted that 'even where a measure is properly directed at a legitimate aim, it may not be regarded as 'necessary' if it produces second-order consequences that 'undermine its likely efficacy'.[287] It should be noted that at no point in the Inquiry's report were 'second-order consequences' ever discussed or elaborated upon. As foreshadowed earlier in the discussion of privacy literature (and referred to in relation of Solove's Taxonomy of Privacy Problems TPPs as Secondary Use), the notion of second-order consequences are a significant concern arising out of metadata retention. Second-order consequences refer to consequences that are an unforeseen or unintended result of an action. In this instance, second-order privacy risk is plainly seen with reference to long-term collection of personal information and resulting profiling capabilities.[288] Considering Solove's reference to Secondary Use of retained metadata will allow for that information to be used in ways that are currently unknown, unknowable or presently unforeseeable. What is known, is that apart from metadata being used to conduct serious criminal and national security investigations, it is also being used to target whistleblowers and to gather information on journalists and their sources.[289]

The discussion of second-order consequences highlights one of Solove's key TPPs – the notion of secondary use: where there are impacts of the collection of personal information, in this case - metadata, that have not been foreseen by the individual whose data is being collected. This personal information is used for purposes that have not been consented to and could potentially be damaging to the individual. In this instance, metadata collected for telecommunications service provider's business purposes is being retained and used for other purposes – on occasion, even for purposes that may generously be termed as grey areas under existing legislation.

For instance, the media have reported that the AFP has recently sought access to a doctor's metadata in order to identify whether the doctor had spoken to a journalist following disclosure of records pertaining to a death in an Australian off-shore detention facility.[290] An argument has been made that the real target of the investigation was the journalist who broke the story, with the doctor whistleblower being targeted because there were fewer legal hurdles to surmount to obtain the

[286] Ibid 27-8 [2.63]-[2.65], [2.67]-[2.69].
[287] Ibid 46 [2.129].
[288] Gökhan Bal and Kai Rannenberg, 'Supporting User Control for Privacy by Advancing Privacy Transparency: The Case of Smartphone Apps' (Paper presented at the European Parliament Science and Technology Options Assessment: Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, Brussels, 08 December 2015 to 09 December 2015) 2.
[289] George Tomossy, Zara Bending and Paul Maluga, 'Privacy and metadata: The hidden threat to whistle-blowers in public health systems' (2017) 3 *Ethics, Medicine and Public Health* 124, 129-130.
[290] Paul Farrell, 'Australian police accessed phone records of asylum whistleblower', *The Guardian (Australian Edition)* (online), 24 May 2016 <https://www.theguardian.com/australia-news/2016/may/24/australian-police-accessed-phone-records-of-asylum-whistleblower>.

doctor's metadata in comparison with obtaining the journalist's metadata.[291] Indeed, the threat of the use of metadata to target whistleblowers under the guise of enforcing the criminal law was evident in the AFP's investigation regarding politically embarrassing leaks that took place mid- to late-2016. These leaks, relating to some negative aspects of the National Broadband Network, resulted in an AFP investigation that led to the AFP raiding Labour Parliamentary offices looking for information about the leaker.[292] It has been argued that the investigation, spanning months and costing significant taxpayer funds for arguably little gain – the identity of a whistleblower – was politically motivated. If that is the case, then far from being used to investigate serious crime and threats to national security, the metadata regime is instead being used to stifle potential dissent in society and to diminish the potential for honest and informed political debate.

The issue of the secondary use of retained metadata is further illustrated by the potential use of metadata in civil proceedings. This concern was raised by the 2015 PJCIS Inquiry where it was noted that the use of metadata in civil proceedings goes against the stated intention of the legislation and will allow metadata to be used for purposes for which the legislation was not designed.[293] The Inquiry found that as the legislation was being specifically enacted for serious criminal law enforcement and national security purposes, it would inappropriate to allow this information to be used in civil proceedings.[294] Nonetheless and despite the recommendations of the 2015 PJCIS Inquiry, between late December 2016 and 27 January 2017, the Federal Attorney-General's Department issued a consultation paper regarding the possibility of using metadata retained that was retained for purposes of investigating and prosecuting serious criminal and national security offences, in civil proceedings. Entitled *Access to Telecommunications Data in Civil Proceedings*, the Attorney-General's Department initiated this consultation process over the Christmas period, when most people would be enjoying their holiday breaks. Despite this, over 200 submissions were made, with significant concern being raised over the possibility of the retained metadata being used outside the purpose for which it was originally retained. Indeed, in October 2014 when the Bill was first introduced to Parliament, the AFP Commissioner indicated that the metadata retention regime will likely be used to target copyright infringements and piracy.[295] Victoria's Commissioner for Privacy and Data Protection made a submission in response to the consultation paper stating that the use of retained metadata should only be permitted in the most serious of circumstances, and that its use in civil proceedings

[291] Tomossy, Bending and Maluga, above n 286, 130.
[292] Seamus Byrne, ''Unprecedented' AFP raid on Labor offices over NBN leaks', *CNET* (online), 20 May 2016 <https://www.cnet.com/au/news/afp-raid-labor-offices-nbn-leaks-election-conroy/>; Rae Johnston, 'NBN Investigation: Australian Federal Police to Raid Parliament Again', *Gizmodo* (online), 24 August 2016 <https://www.gizmodo.com.au/2016/08/nbn-investigation-the-australian-federal-police-to-raid-parliament-again/>.
[293] Parliamentary Joint Committee on Intelligence and Security, above n 202, 216-224.
[294] Ibid 223 [6.115]-[6.116].
[295] Allie Coyne, 'AFP will use data retention to fight piracy', *IT News* (online), 30 October 2014 <https://www.itnews.com.au/news/afp-will-use-data-retention-to-fight-piracy-397367>.

falls significantly short of this standard, that 'it is difficult to conceive of a civil matter of such consequence as to necessitate access to what is effectively a comprehensive surveillance system'.[296]

The potentialities of the limits of secondary uses of retained metadata have been made even starker when late in March 2017, the United States Congress voted to allow telecommunications service providers to sell their subscribers' data, including browser history.[297] There is no immediate risk of telecommunications service providers being able to follow suit in Australia as it would currently be in breach of the Privacy Act and there is no discussion of making the necessary legislative amendments to allow this to take place. However, given the misrepresentation of the purpose of metadata retention that took place — whereby retained metadata would be used only for the investigation of serious crimes and threats to national security — and given the severity of the potential impacts upon individuals, even the potential of such an extension of secondary use purposes of retained metadata must be considered a concern. The resulting insecurity and feelings of invasion of privacy that an individual may feel with respect to their metadata are, incidentally, another one of Solove's TPPs that is negatively impacted by this legislation - namely, Intrusion.

While discussing the TPP of Insecurity, Solove focused on the notion of unauthorised third parties having access to personal information; he did so by focusing on the concept of identity theft. Insecurity is related to Aggregation and Identification in the sense that data is collected and stored, and is able to be linked directly to individuals. Insecurity arises when there is unauthorised use of the stored data. There have been many instances of unauthorised use or disclosure, intentional or inadvertent, of personal information in recent years, but more interestingly, there have been a number of apparent privacy breaches perpetrated by agencies at all levels of government throughout Australia including as recently as 2017. For instance, in March 2017, the Australian Taxation Office (**'ATO**') admitted that it had exposed personal information about their employees to an outside contractor.[298] In order to profile voting patterns during an industrial ballot, the ATO 'covertly supplied its contractor with the names, email addresses, locations of work and pay grades of each of its 19,000 employees without their knowledge or consent', including, in some cases, private emails and home addresses.[299] The ATO has not admitted wrongdoing and it does not appear that the matter has been reported to the Office of the Australian Information Commissioner or any other relevant body, but at

[296] David Watts, Victorian Commissioner for Privacy and Data Protection, Submission to the Attorney-General's Department, Parliament of Australia, *Access to Telecommunications Data in Civil Proceedings*, 27 January 2017, 2.

[297] Olivia Solon, 'Your browsing history may be up for sale soon. Here's what you need to know', *The Guardian (Australian Edition)* (online), 28 March 2017 <https://www.theguardian.com/technology/2017/mar/28/internet-service-providers-sell-browsing-history-house-vote>.

[298] Noel Towell, 'Busted: Australian Taxation office exposed voter-profiling its own public servants during industrial ballot', *The Canberra Times* (online), 14 March 2017 <http://www.canberratimes.com.au/national/public-service/busted-public-services-voter-profiling-exposed-20170310-guv8uy.html>.

[299] Ibid.

face value, this appears to be a grave breach of privacy. In 2015, the Parliamentary Joint Committee on Law Enforcement recommended that the ATO be one of the agencies that should be granted access to retained metadata under the TIA Act to allow the agency to investigate serious fraud and other financial crimes 'for the purpose of the protection of public finances'.[300] This however, did not happen and the ATO is not listed as an agency explicitly permitted to access retained metadata without a warrant. The information they released about their employees was similar in practice to information obtained through metadata retention. Further, there is no protection in the TIA Act to prevent agencies from applying analytics to retained metadata and thereby causing Solove's TPP of Aggregation. As this would arguably form part of ATO's internal data rather than retained metadata, this could have also been released had ATO had access to retained metadata under the TIA Act. All of this is of course speculative, however the issue remains that there is nothing in the TIA Act to prevent such event from occurring. This conclusion was underscored when another Government department purposefully released a client's details to the media.

In late 2016, Centrelink commenced an enhanced programme of reclaiming alleged overpayments of benefits. The method used to calculate overpayments and the manner by which Centrelink, an agency within the Department of Human Services, contacted the affected clients resulted in much controversy and many disputed claims. One such dispute was with a past recipient Andie Fox who wrote an article detailing her experience dealing with the agency and the third-party debt collection agency contracted to recover alleged overpayments.[301] On 26 February 2016 however, another article was published detailing Centrelink's interactions with Ms Fox, including her claim history.[302] Centrelink confirmed that they had approved the release of Ms Fox's information, claiming it was 'necessary to correct the public record' about several alleged inaccuracies in Ms Fox's statement.[303] The secretary for the Department of Human Services claimed that the disclosure was legally permitted, citing discretionary powers under the *Social Security (Administration) Act 1999* (Cth) to disclose information 'if the Secretary certified that it is necessary in the public interest to do so'.[304] The initial disclosure was compounded days later when an internal memo containing additional

[300] Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into Financial Related Crime* (2015) 21-2 [3.7].
[301] Andie Fox, 'As a struggling single mother, Centrelink terrorised me over ex-partner's debt', *The Canberra Times* (online), 06 February 2017 <http://www.canberratimes.com.au/lifestyle/life-and-relationships/real-life/as-a-struggling-single-mother-centrelink-terrorised-me-over-expartners-debt-20170205-gu61nu.html>.
[302] Paul Malone, 'Centrelink is an easy target for complaints but there are two sides to every story', *Sydney Morning Herald* (online), 26 February 2016 <http://www.smh.com.au/comment/centrelink-is-an-easy-target-for-complaints-but-there-are-two-sides-to-every-story-20170224-gukr4x.html>.
[303] Christopher Knaus and Paul Farrell, 'Centrelink recipient's data released by department to counter public criticism', *The Guardian (Australian Edition)* (online), 27 February 2017 <https://www.theguardian.com/australia-news/2017/feb/27/centrelink-recipients-data-released-by-department-to-counter-public-criticism>.
[304] *Social Security (Administration) Act 1999* (Cth) s 208(1)(a).

personal information relating to Ms Fox was mistakenly sent to reporters.[305] The initial disclosure has now been referred to the AFP for investigation of any wrongdoing by the person who authorised the disclosure.[306] The issue at stake here is that a Government department is releasing personal information of an individual who is critical of the department's actions; the resulting insecurity falls within the meaning of Solove's TPP due to the fact that the unauthorised use of personal information creates fear for anyone who would criticise the Government. While these examples do not pertain to metadata directly, they demonstrate not only the capacity but indeed proven instances where the Australian Government has utilised personal information for Secondary Uses within the meaning of Solove's TPP. Moreover, these matters raise the spectre of Solove's TPP of Disclosure, whereby information was seemingly disclosed or made public for malicious or ulterior motives, both in relation to the ATO release of employee information and the Centrelink release of Ms Fox's information.

(c) Is Metadata Retention a Proportionate Response to the Outlined Threat?

For a legal measure to be considered a proportionate response it must infringe the right to individual privacy only so far as necessary to achieve a legitimate aim. The Revised Explanatory Memorandum acknowledged that the retention of metadata interferes with the right to privacy and freedom of expression as protected under the *International Covenant on Civil and Political Rights.*[307] The 2015 PJCIS Inquiry also noted that the decision of the *Digital Rights Ireland Case* provides useful guidance in determining the issue of proportionality. This usefulness is particularly pertinent given that the Directive served as the model for Australia's metadata retention laws.[308] The Court in the *Digital Rights Ireland Case* stated that:

> Any limitation on the exercise of the rights and freedoms laid down by the [Charter of Fundamental Rights of the European Union] must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the [European Union] or the need to protect the rights and freedoms of others.[309]

---

[305] Christopher Knaus, 'Exclusive: minister's office sent journalist internal briefings about Centrelink client', *The Guardian (Australian Edition)* (online), 02 March 2017 <https://www.theguardian.com/australia-news/2017/mar/02/exclusive-ministers-office-sent-journalist-internal-briefings-about-centrelink-client>.
[306] 'Minister referred to police over release of Centrelink details', *The New Daily* (online), 02 March 2017 <http://thenewdaily.com.au/news/national/2017/03/02/minister-referred-police-release-centrelink-details/>.
[307] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 12.
[308] Parliamentary Joint Committee on Intelligence and Security, above n 202, Appendix A.
[309] Ibid 61 [2.180]. Article 7 of the *European Charter of Fundamental Rights of the European Union* closely resembles article 17(1) of the *International Covenant on Civil and Political Rights*, dealing as it does with the protection of person from unlawful or arbitrary interference with his or her privacy, home, family or communications; article 8 of the Charter deals with the protection of personal data – an issue legislated into the *Privacy Act 1988* (Cth).

As noted above, the requirements regarding privacy protection interpreted by the Court in the *Digital Rights Ireland Case* represent best-practice of privacy protection.[310] The *Digital Rights Ireland Case* established a number of factors by which the Court was able to gauge the proportionality of the Directive. The Court said that for a law seeking to retain metadata to be considered proportionate, it must:

1. Be 'provided for by law';[311]
2. Respect 'the essence to the right of privacy in that it [does] not allow access to content of communications';[312]
3. Respect 'the essence of the right to the protection personal data';[313] and
4. Satisfy 'the test of the objective of general interest in promoting investigations into international terrorism and organised crime'.[314]

To further its position advancing the metadata regime, the Australian government asserted that the proportionality of the metadata retention regime cannot be considered in isolation to its purported purpose, which is to retain individual metadata in order to advance criminal and national security investigations.[315] Submissions in favour of the metadata retention regime made reference to the report of the United States' National Research Council entitled *Bulk Collection of Signals Intelligence: Technical Options*, which concluded that 'there are no technical alternatives that can accomplish the same function as bulk collection and serve as a complete substitute for it'.[316] This was the argument put forward by the Australian Attorney-General's Department in relation to the question why the Government had not considered the enlargement of existing preservation order scheme, stating that '[e]vidence cannot be preserved if it was never retained, or if it has already been deleted'.[317] The AFP states that 'without data retention, agencies would frequently lack the necessary information to identify a suspect and serve a preservation notice...[i]n many instances, the role that [metadata] place [*sic*] in the early stages of investigations is to assist in attribution'.[318] The Attorney-General's Department further noted that the viability of preservation orders being a substitute for bulk metadata retention was examined by a number of other jurisdictions, including the Council of Europe

[310] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014).
[311] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [38].
[312] Ibid [39].
[313] Ibid [40].
[314] Ibid [42]-[44].
[315] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 12.
[316] Parliamentary Joint Committee on Intelligence and Security, above n 202, 55-56 [2.165].
[317] Ibid 58 [2.171].
[318] Ibid 59 [2.174].

and the European Commission. Each of these reviews reportedly concluded that preservation orders made for prospective metadata were not a 'substitute for accessing existing [metadata]'.[319]

However, the impact upon individual privacy that results from a blanket and ubiquitous retention of metadata has a disproportionate impact upon individuals. Both the New South Wales Council for Civil Liberties and the Institute of Public Affairs made submissions to the 2015 PJCIS Inquiry as to the value of privacy in a civil, democratic society.[320] The value of privacy to the individual was discussed earlier in this document. For instance, the collection of metadata has the potential to amount to ubiquitous government surveillance, impacting upon freedom of expression.[321] Referred to by Solove as the privacy problems of Aggregation and Identification, the Victorian Commissioner for Privacy and Data Protection noted that the collection of metadata can reveal:

> [P]atterns of communications that will enable those who have access to it to investigate and understand the private lives of all Australians, such as the habits of everyday life, places of residence, minute by minute movements, activities undertaken, social, professional and commercial arrangements, and relationships and social environments frequented.[322]

In fact, researchers at the Massachusetts Institute of Technology conducted a study regarding the re-identifiability of the individual based on anonymised credit card information.[323] The study showed that with a single source — credit cards — having merely four distinct points of metadata comparison allowed researcher to re-identify anonymised individuals with 90% accuracy.[324] Closer to home, in 2016 the University of Melbourne conducted an experiment to examine the impact of the metadata retention laws upon individual privacy. The experiment involved 12 teams of children sifting through a dataset of metadata of the sort retained pursuant to the retention regime with the help of filtering software. The aim was to track a hypothetical corporate whistleblower on the basis of two points of information – the topic of the disclosed information (fracking chemicals) and the email address of the recipient of the documents (a non-governmental organisation). All but one team was able to identify the fictional whistleblower, and the winning team completed the task in an hour.[325]

Thus, the assertion that metadata is somehow less privacy-intrusive than access to traffic and location data comparators — a position propagated by the Government[326] — is problematic for several reasons. Firstly, as noted by Professor Triggs, '[a] great deal can be learned from metadata. Indeed, in

---

[319] Ibid 59 [2.176].
[320] Ibid, 49-50 [2.140]-[2.141]
[321] Ibid 50 [2.142].
[322] Ibid 50 [2.143].
[323] de Montjoye et al, above n 100.
[324] Ibid 537.
[325] James Purtill, 'How pre-teens using metadata found a whistleblower in two hours', *ABC News* (online), 12 December 2016 <http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whisteblower-using-metadata/8113668>.
[326] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 14.

many cases, more can be learned from metadata than can be learned from content'.[327] In their submissions to the Inquiry, the Electronic Frontiers Australia and the Australian Privacy Foundation referred to the *Digital Rights Ireland Case*.[328] In this case, the Court found:

> Those [metadata], taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary residences, daily or other movements, the activities carried out, the social relationships of those person, and the social environments.[329]

Secondly, while it is debatable which is more privacy-intrusive — traffic, content and location data, or metadata — it is, in practice, a moot point. Through the processes of Aggregation and Identification, the nature of content can easily be inferred through the collection and analysis of metadata. Moreover, it is disingenuous to assert that location and content are separate issues as, under the TIA Act, location data is collected.[330]

The former Chair of the Australian Privacy Foundation stated that the metadata retention regime amounts to mass surveillance in Australia. The matter, he says, moves beyond personal, targeted surveillance into the realm of mass surveillance due to the pervasive nature of the retention.[331] The Vice Chair of the Australian Privacy Foundation argued in his submission, that the law would have a disproportionate impact and is a 'sledgehammer that unjustifiably breaches the right to privacy [of those] who are overwhelmingly neither criminals nor terrorists'.[332] He goes on to cite from the report prepared by the United Nations' Special Rapporteur on the Promotion and Protection on the Right to Freedom of Opinion and Expression noting:

> Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party [metadata] retention...appears neither necessary nor proportionate.[333]

In fact, there is reason to fear that the Australian Government may use available information and data about individuals for political purposes, not just for the purposes of investigating and prosecuting serious crimes and threats to national security. Solove discussed the potential for unauthorised use and disclosure of personal information as a problem stemming from Aggregation and Identification, leading to Insecurity of the individual; these TPPs have all been witnessed with respect to personal information in recent months. For instance, the release of Ms Fox's personal information is clearly a breach of her privacy, yet it was authorised under law. It is not within the

---

[327] Parliamentary Joint Committee on Intelligence and Security, above n 202, 54 [2.159].
[328] Ibid Appendix A.
[329] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [27].
[330] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187AA(1).
[331] Parliamentary Joint Committee on Intelligence and Security, above n 202, 53 [2.153].
[332] Ibid 51 [2.146].
[333] Ibid 51 [2.146].

scope of this research to examine the fundamental legality of the actions of the responsible decision-maker, but on the face of the matter, releasing personal information to stifle dissent would clearly have an impact on the willingness of others to question the authority of the Government – something that was discussed previously as a fundamental reason for why privacy must be protected in a democratic society. There is concern that the intention behind the release of Ms Fox's information was meant to discredit her and effectively silence her from speaking out against the Government.[334] If proven to be illegal, this incident would bode ill for the security of the retained metadata of millions of people and would have the potential to cause a massively disproportionate impact on the persons whose metadata has been retained.

This is also not yet turning the attention to disclosures that have not been authorised under law. In late March 2017, it became known that a Queensland police officer abused his authority to access a secure database to check the personal details of unnamed persons without lawful authority.[335] The unauthorised access of personal information from secure databases is a problem Australia-wide,[336] where police officers have used their respective databases to look up the personal information of celebrities,[337] and stalking of individuals a police officer met through a phone dating service.[338] Worryingly, the prevalence of such unauthorised access is unknown or undisclosed, and when matters do become public knowledge, little information is usually provided.[339] Further still, the above does not account for inadvertent disclosure,[340] nor does it account for malicious hacking of databases, both of which are issues that would affect the impact of the metadata retention regime, and therefore, its proportionality under international law.

In their submission to the 2015 PJCIS Inquiry, the Federal Attorney-General's Department identified the following issues as being the reason why the Court in the *Digital Rights Ireland Case* reached a decision that the Directive lacked proportionality:

---

[334] Zeb Holmes, *Centrelink's Release of Critic's Personal Information May Be a Crime* (10 April 2017) Sydney Criminal Lawyers < http://www.sydneycriminallawyers.com.au/blog/centrelinks-release-of-critics-personal-information-may-be-a-crime/>.

[335] Allie Coyne, 'Qld cop charged with misusing database', *IT News* (online), 21 March 2017 <https://www.itnews.com.au/news/qld-cop-charged-with-misusing-database-455534>.

[336] Queensland, Victoria and New South Wales have all been impacted in recent years.

[337] 'Australia captain's private details allegedly accessed by police', *The New Daily* (online), 17 February 2017 <http://thenewdaily.com.au/sport/other-sports/2017/02/17/laura-geitz-police/>.

[338] Allie Coyne, 'Qld Police officer charged with hacking force database', *IT News* (online), 22 June 2016 <https://www.itnews.com.au/news/qld-police-officer-charged-with-hacking-force-database-421133>.

[339] See, eg, Tammy Mills, 'Police officer charged with unauthorized access to LEAP database', *The Age* (online), 20 may 2015 <http://www.theage.com.au/victoria/police-officer-charged-with-unauthorised-access-of-leap-database-20150520-gh5tzj.html>.

[340] See, eg, Tom McIlroy, Fergus Hunter and Rania Spooner, 'Red Cross data leak: personal data of 550,000 blood donors made public', *The Sydney Morning Herald* (online), 28 October 2016 <http://www.smh.com.au/federal-politics/political-news/red-cross-data-leak-personal-data-of-550000-blood-donors-made-public-20161028-gscwms.html>.

1. The Directive, in a generalised manner, 'cover[ed] all persons and all means of electronic communications as well as all traffic [metadata] without any differentiation, limitation or exception';
2. The Directive did not lay down objective criteria to determine the limits of access of competent or designated authorities to retained metadata;
3. Required that the metadata be retained for a period of at least six months, 'without any distinction being made between the categories of data';
4. The Directive did not 'provide for sufficient safeguards...to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data'; and
5. The Directive did not require the data to be retained within the European Union.[341]

The Court also found that the Directive did not provide for 'irreversible destruction of [metadata] at the end of the retention period'.[342] While it is clear that the European Commission turned their mind to the destruction of the retained data at the end of the retention period,[343] the Court concluded that the provisions were inadequate to ensure that the destruction would be 'irreversible'. In implementing the metadata retention regime into the TIA Act, the Australian Parliament failed to ensure that metadata would be destroyed at all – the current version of the TIA Act contains no provisions requiring the destruction of the retained metadata at the end of the retention period. The Australian telecommunications service providers may retain the stored metadata indefinitely at their discretion, destroying it only if they 'no longer need it'.[344]

Moreover, the Court in the *Digital Rights Ireland Case* also noted that 'there is no provision in the Directive that the access to data be restricted for the purposes of preventing serious crime or the conduct of prosecutions'.[345] Critique of this limitation is enhanced by a key factor in the Court's reasoning that the Directive:

> [Did] not require any relationship between the [metadata]...and a threat to public security and, in particular, it is not restricted to a retention in relation
>
> > (i) [T]o data pertaining to a particular time period and/or a particular geographic zone and/or to a circle of particular person likely to be involve, in one way or another, in a serious crime, or

[341] Parliamentary Joint Committee on Intelligence and Security, above n 202, 62 [2.183].
[342] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [67].
[343] *Directive 2006/24/EC/ of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54, art 7(d).
[344] Selvadurai, above n 261, 40.
[345] *Digital Rights Ireland Case* (C-293/12) [2014] ECJ 238, [67].

> (ii) [T]o person who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[346]

As noted previously, the only restriction on the use of retained metadata by authorised agencies is that it is reasonably necessary for the purpose of law enforcement. This aspect of the Australia's metadata retention laws has already been discussed in an earlier section – while this test may place some limitation on access, it is wholly inadequate in light of the fact that to retain prospective metadata requires the investigation of a serious criminal offence. There is little in the TIA Act limiting the collection of metadata to persons or geographic locales that are relevant to specific serious criminal or national security operations. The Court grounded their findings in a lack of objective criteria ensuring that data being collected is formulated so as to be 'precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary' to be retained.[347] This included the lack of consideration concerning any consideration as to the usefulness or for purpose of the metadata retention periods.[348] These key factors in the Court's reasoning were missed by the Federal Attorney-General in their submission to the Inquiry as to the outcome of the *Digital Rights Ireland Case*.

In reading the decision in the *Digital Rights Ireland Case*, it becomes clear that the Court decided against the continued implementation of the metadata retention regime envisaged by the Directive on the grounds that it failed to meet the requirement of proportionality. The Court made the determination that 'by adopting Directive 2006/24, the [European Union] legislature has exceeded the limits imposed by compliance with the principle of proportionality'.[349] Given the common origins of the Directive and Australian's metadata retention laws and the authoritative nature of the Court's decision on the application of international law protecting individual privacy, the flaws identified by the Court in the *Digital Rights Ireland Case* — both with respect to the issue of proportionality and the procedural aspects of the laws' practical implementation — should have been addressed to ensure that Australia was complying with the standards of best-practice in protecting individual privacy. It does not appear that this process of remediation took place, as many of the flaws intrinsic to the Directive have been ported to the Australia's metadata retention law. In much the same manner as in the *Digital Rights Ireland Case*, the implementation of the Australian metadata retention regime is wider than is necessary to meet the legitimate aim of this legislation. This is the case for the following reasons:

1. The retention of metadata includes every person and every mode of telecommunications in Australia, with no differentiation, limitation or exception;

[346] Ibid [59].
[347] Ibid [64]-[65].
[348] Ibid [63].
[349] Ibid [69].

2. Under the metadata retention regime, there are no objective criteria that can be used to determine whether access to retained metadata is necessary and appropriate. This became an issue in light of the only requirement for access to retained metadata being that it is 'reasonably necessary' for the purposes of law enforcement;
3. The data is to be retained for a minimum period of two years, whereas the Court in the *Digital Rights Ireland Case* suggested that the Directive's retention requirement of six months to two years was too extensive;
4. There is no requirement to irrevocably destroy the metadata retained under the regime upon the expiration of the retention period;
5. Under the metadata retention regime, there is no requirement for any specific investigation or security threat and the requirement to retain an individual's metadata; and
6. There is no requirement to retain the collected metadata within Australia.

Additionally, while the metadata retention regime requires the stored data to be encrypted, it does not provide any guidance or minimum specifications to ensure effective security.[350] This privacy concern, combined with the previous point that retained metadata is not required to be stored in Australia, exposes the sensitive personal information that is metadata to significant privacy threats. The Government readily admits that it has no way of knowing how much of the retained metadata is currently being stored extrajurisdictionally as there is no provision in the legislation requiring this disclosure.[351] It is not difficult to imagine that the retained metadata may be stored in a jurisdiction with lax privacy protections where, upon the expiration of the two year minimum retention period metadata, the metadata may be sold – either to recover the costs of establishing the retention system or simply for profit. The precedent for the selling of such personal information has already been set in the United States earlier this year;[352] it is not difficult to imagine a profits-driven corporation examining this possibility considering the lack of any relevant restriction that can apply internationally. This, coupled with the preceding analysis, ensures that the impact of this legislation is not proportionate; that is – it cannot be shown that the metadata retention regime as legislated in

[350] Selvadurai, above n 261, 40.
[351] Allie Coyne, 'AGD blind to offshore storage of Aussie metadata', *IT News* (online), 6 February 2017 <https://www.itnews.com.au/news/agd-blind-to-offshore-storage-of-aussie-metadata-451432>.
[352] Solon, above n 294; Libby Watson, 'US Congress Just Gave Internet Providers The Green Light To Sell Customers' Browsing History Without Consent', *Gizmodo* (online), 29 March 2017 <https://www.gizmodo.com.au/2017/03/us-congress-just-gave-internet-providers-the-green-light-to-sell-customers-browsing-history-without-consent/>; Tom Wheeler, 'How the Republicans Sold Your Privacy to Internet Providers', *The New York Times* (online), 29 March 2017 <https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html?_r=0>; Brian Fung, 'What to expect now that Internet Providers can collect and sell your Web browser history' *The Washington Post* (online), 29 March 2017 <https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?utm_term=.d5b1538b0523>.

Australia is, to borrow the phrasing of the Office of the United Nations High Commissioner for Human Rights, 'necessary for reaching a legitimate aim...and the least intrusive option available'.[353]

VI Conclusion

Within the context of the Third Wave of privacy discourse and examined in light of Solove's TPPs, mandatory and ubiquitous metadata retention applies to all four identified categories of privacy problems. The retention of metadata gives rise to the problem of Surveillance, whereby any person in Australia can be monitored. Further, through structured analysis of retained metadata by way of Aggregation, Identification of the individual is possible even when metadata is seemingly anonymised; this allows for Secondary Use of information beyond the purposes for which it was originally retained and leads to the problem of Insecurity of the individual whose metadata was retained. Moreover, recent events indicate that Disclosure and Invasion are distinct privacy problems in Australia. While these events did not relate specifically to metadata, they illustrated a particular lack of regard towards privacy protection by the Australian Government in relation to personal information generally. This political reality does not bode well for metadata protection, particularly given that metadata is a rich source of individual and collective information. With a view to the distribution, prevalence, and pervasiveness of technology, the Third Wave calls for greater awareness of the potential for privacy intrusions that are inherent with modern technology, and in relation to metadata, are also invisible. This ever-expanding reliance on technology manifests an increasingly vital examination and reaffirmation of international standards of privacy protection and a need to ensure that these standards are rigorously complied with. Having examined Australia's TIA Act, this dissertation concludes that the legislation fails to meet the standards of privacy protection required under article 17 of the ICCPR.

This dissertation examined the TIA Act and related material and analysed it against the requirements of privacy infringements under article 17 of the ICCPR. The legal test relating to article 17 centres around three prongs – for a law aimed at infringing the right to privacy to be lawful under international law, it must: (i) be necessary to fulfil a legitimate aim; (ii) be effective in achieving that aim; and (iii) not enlist measures that disproportionately burden or intrude on the right to privacy against the aim sought. There is room for disagreement whether Australia's metadata retention regime meets the requirements of necessity and effectiveness, but it certainly fails the test of proportionality. The legislation as passed was intended to achieve the legitimate aim of ensuring the safety and protection of society against serious crimes and threats to national security. However, there is considerable debate as to whether mandatory and ubiquitous metadata retention is both

[353] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) [23].

necessary and effective at achieving this aim. The lack of empirical evidence of efficacy of mandatory metadata retention in aiding criminal or national security investigations leads to the conclusion that it is not effective and thus, not necessary; furthermore, the way in which the legislation has been put to use since its enactment — pursuing minor criminal offending and investigating whistleblowers — further suggests that the law is not necessary. Moreover, a secondary purpose of the legislation — limiting the number of agencies who have access to retained metadata — is being circumvented in a number of ways, suggesting that the legislation is not effective. Additionally, as discussed above, the way in which metadata is subject to potential threats of Aggregation, Identification, Secondary Use, Disclosure, and Intrusion all lead to the conclusion that the impact upon the privacy of the individual is highly disproportionate.

Privacy is a vital and dynamic concept that impacts upon many aspects of our daily lives, which will continue to evolve and to adapt to future technological developments. The fundamental failings of Australia's metadata retention under article 17 of the ICCPR, arise primarily in the Act's drafting (which took place against a political backdrop wherein the protection of individual privacy interests did not evidently present a priority for the Australian Government), with associated incongruities in its implementation and enforcement. This resulted in the Government not taking concrete action when the limitations of the metadata retention regime were pointed out; this is also evident with respect to the recent privacy breaches that appear to be perpetrated by Australian Government. As a remedy to this underlying problem, the Australian Government should, in the first instance:

1. Decrease the retention period from two years to six months to one year;
2. Implement amendments to the TIA Act to strengthen and broaden the role of the Public Interest Advocate to allow examination of all requests for access to retained metadata;
3. Remove the current ambiguity and opaqueness from the legislation and ensure that principles of procedural fairness are followed in all circumstances;
4. Ensure that there exists a system of robust, independent oversight of the system in granting access to retained metadata to agencies, a decision that should be made by a senior justice of an Australian Federal Court;
5. Ensure that metadata is only accessibly for the investigation and prosecution of serious criminal offences and threats to national security, strictly defined in scope of the offences, and the geographic and temporal relationship between the metadata sought and the event in question;
6. There must be clear, stated, and objective criteria by which limits of access to metadata may be determined;
7. Ensure that the retained metadata will always be contained within the geographical locale of Australia; and

8. Ensure that upon the expiration of the retention period, the retained metadata is permanently destroyed.

Further, given the continual development of technology, its impact in the Third Wave and beyond is increasingly difficult to predict except to say that inevitably, privacy interests will be increasingly under threat from new and evolving technology. To ensure that privacy is adequately protected and to indicate its commitment to privacy protection, the Australian Government should formally recognise the individual right to privacy within the meaning of article 17 of the ICCPR. This may be achieved by implementing a Federal Charter of Rights or more fully ratifying article 17 of the ICCPR into Federal legislation by way of a statutory tort of invasion of privacy.

VII REFERENCES

A *Articles/Books/Reports*

Adams, Elbridge, 'The Right of Privacy, and its Relation to the Law of Libel' (1905) 39 *American Law Review* 37

Altman, Irwin, *The Environment and Social Behaviour: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole Publishing Co, 1975)

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

Bal, Gökhan and Kai Rannenberg, 'Supporting User Control for Privacy by Advancing Privacy Transparency: The Case of Smartphone Apps' (Paper presented at the European Parliament Science and Technology Options Assessment: Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, Brussels, 08 December 2015 to 09 December 2015)

Banisar, David, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments*, (5 May 2008) Privacy International <www.privacyinternational.org/survey/phr2000/overview.html>

Banisar, David and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18 *John Marshall Journal of Computer and Information Law* 1

Bennett, Colin, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992)

Bratman, Benjamin, 'Brandeis and Warren's *The Right to Privacy* and the Birth of the Right to Privacy' (2001-2002) 69 *Tennessee Law Review* 623

Bruyer, Richard, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553

Capurro, Rafael, 'Privacy. An intercultural perspective' (2005) 7(1) *Ethics and Information Technology* 37

Clarke, Roger, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7 *Information Technology & People* 6

Cohen, Julie, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373

Cooley, Thomas, *Cooley on Torts* (2nd ed, 1888)

DeCew, Judith, 'Privacy' in Edward Zalta (ed), *Stanford Encyclopedia of Philosophy* (Stanford University, 2006) <http://plato.stanford.edu/entries/privacy/>

Digglemann, Oliver and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441

Dixon, Martin, *Textbook on International Law* (Oxford University Press, 7th ed. 2013)

Donner, Frank, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System* (Knopf, 1983)

European Commission*, Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* [2011]

Foucault, Michel, *Discipline & Punish: The Birth of the Prison* (Vintage Books, 1995) 200 [trans of: *Surveiller et Punir* (first published 1975)]

Franzen, Jonathan, *How to Be Alone* (Picador, 2003)

Fuchs, Christian, 'Towards an alternative concept of privacy' (2011) 9(4) *Journal of Information Communication and Ethics in Society* 220

Gavison, Ruth, 'Privacy and the Limits of Law' (1980) 89(3) *Yale Law Journal* 421

Gillion, John, *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy* (Chicago University Press, 2001)

Glendon, Mary Ann, 'Knowing the Universal Declaration of Human Rights' (1998) 73(5) *Notre Dame Law Review* 1153

Glendon, Mary Ann, 'The Rule of Law in the Universal Declaration of Human Rights' (2004) 2(1) *Northwest Journal of International Human Rights* 1

Gross, Hyman, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34

Groves, Matthew, 'Substantive legitimate Expectations in Australian Administrative Law' (2008) 32 *Melbourne University Law Review* 470

Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror* (Scribe Publications, 2002)

Hoffman, Bruce, *Insider Terrorism* (Victor Gollancz, 1998)

Inness, Julie, *Privacy, Intimacy, and Isolation* (Oxford University Press, 1992)

Leonard, Peter, 'Mandatory internet data retention in Australia: Looking the horse in the mouth after it has bolted' (2015) 101 *Journal of the Intellectual Property Society of Australia and New Zealand* 43

Lindsay, David, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29(1) *Melbourne University Law Review* 131

Lyons, David, *The Electronic Eye: The Right of Surveillance Society* (Polity Press, 1994)

Magi, Trina, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' (2011) 81(2) *The Library Quarterly* 187

Mill, John Stuart, *Utilitarianism, Liberty and Representative Government* (J.M. Dent & Sons Ltd, 1964)

Miller, Arthur, *The Assault on Privacy* (University of Michigan, 1971)

de Montjeye, Yves-Alexandre et al, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347(6221) *Science* 536

Nowak, Manfred, *UN Convention on Civil and Political Rights: CCPR Commentary* (N.P. Engel, 1993)

Oulasvirta, Antti, et al, 'Long-Term Effects of Ubiquitous Surveillance in the Home' (Paper presented at the 14th International Conference on Ubiquitous Computing, Pittsburgh, USA, 05 to 08 September 2012)

Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of Legislation in Accordance with the Human Rights (Parliamentary Scrutiny) Act 2011*, 15th Report, 44th Parliament (November 2014)

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (February 2015)

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source* (March 2015)

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)

Penney, Jonathan, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) *Berkeley Technology Law Review* 117

Pitt, William, *Speech on the Excise Bill*, House of Commons, Parliament of the United Kingdom (March 1763)

Post, Robert, 'Three Concepts of Privacy' (2011) 89 *Georgetown Law Journal* 2087

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

Rosen, Jeffrey, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random house, 2004)

Selvadurai, Niloufer, 'The Retention of Telecommunications Metadata: A Necessary National Security Initiative or a Disproportionate Interference with Personal Privacy?' (2017) 23(2) *Computer and Telecommunications Law Review* 35

Shaw, Thomas, *World War II Law and Lawyers: Issues, Cases, and Characters* (ABA Book Publishing, 2013)

Simmel, Arnold 'Privacy' (1968) 12 *International Encyclopedia of the Social Sciences* 480

Smith, Jeff, *Managing Privacy: Information Technology and Corporate America* (Southern Economic Association, 1994)

Solove, Daniel, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087

Solove, Daniel, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477

Solove, Daniel, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745

Solove, Daniel, *Understanding Privacy* (Harvard University Press, 2008)

Stephen, James Fitzjames, *Liberty, Equality, Fraternity* (first published 1873; Cambridge University Press, 1967)

Stewart, Daniel, 'Protecting Privacy, Property and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd' (2002) 30(1) *Federal Law Review* 177

Stoke, Hugo and Arne Tostensen (eds), *Human Rights in Development Yearbook 1999/2000: The Millennium Edition* (Kluwer Law International, 2001)

Swire, Peter, 'Financial Privacy and the Theory of High-Tech Government Surveillance' (1999) 77 *Washington University Law Quarterly* 461

Tomossy, George, Zara Bending and Paul Maluga, 'Privacy and metadata: The hidden threat to whistle-blowers in public health systems' (2017) 3 *Ethics, Medicine and Public Health* 124

United Nations, *History of the Document* <http://www.un.org/en/sections/universal-declaration/history-document/index.html>

Volokh, Eugene, 'Freedom of Speech and information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You' (2000) 52 *Stanford Law Review* 1049

Warren, Samuel and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193

Westin, Alan, *Privacy and Freedom* (Atheneum, 1967).

Whitman, James, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113(6) *Yale Law Journal* 1151

B *Cases*

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

Dagg v Canada (Minister of Finance) [1997] 2 S.C.R. 403

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (C-293/12) [2014] ECJ 238

DPP v Kaba (2014) 44 VR 526

Elettronica Sicula SpA (ELSI) (United states of America v Italy) (Judgment) [1989] ICJ Rep 15

Entick v Carrington (1795) 95 ER 807

Giller v Procopets [2004] VSC 113 (07 April 2004)

Giller v Procopets (2008) 24 VR 1

Grosse v Purvis [2003] QDC 151 (16 June 2003)

International News Service v Associated Press, 248 US 215 (1918)

Jane Doe v Australian Broadcasting Corporation [2007] VCC 281 (03 April 2007)

Kioa v West (1985) 159 CLR 550

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

Victoria Park Racing and Recreation Grounds Company Limited v Taylor (1937) 58 CLR 479

C *Legislation*

Australian Constitution

Crimes Act 1900 (NSW)

Directive 2006/24/EC/ of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] OJ L 105/54

Privacy Act 1988 (Cth)

Social Security (Administration) Act 1999 (Cth)

Telecommunications Act 1997 (Cth)

Telecommunications (Interception and Access) Act 1979 (Cth)

D *Treaties*

Charter of the United Nations

International Covenant on Civil and Political Rights, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976)

International Covenant on Economic, Social and Cutural Rights, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 03 January 1966)

Optional Protocol on Civil and Political Rights, opened for signature 19 December 1966, 999 UNTS 302 (entered into force 23 March 1976)

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

E *Other*

Anderson, Stephanie, 'List of agencies applying for metadata access without warrant released by Government', *ABC News* (online), 18 January 2016 <http://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836>

Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, Discussion Paper (July 2012)

Attorney-General's Department, Parliament of Australia, *About Us* <https://www.ag.gov.au/About/Pages/default.aspx>

'Australia captain's private details allegedly accessed by police', *The New Daily* (online), 17 February 2017 <http://thenewdaily.com.au/sport/other-sports/2017/02/17/laura-geitz-police/>

Byrne, Seamus, ''Unprecedented' AFP raid on Labor offices over NBN leaks', *CNET* (online), 20 May 2016 <https://www.cnet.com/au/news/afp-raid-labor-offices-nbn-leaks-election-conroy/>

Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12562 (Malcolm Turnbull, Minister for Communication)

Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2126 (Jacinta Collins)

Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2242-2243 (Nick Xenophon)

Commonwealth, *Parliamentary Debates*, Senate, 24 March 2015, 2245 (George Brandis, Attorney-General)

Communications Alliance, Submission to the Attorney-General's Department, Parliament of Australia, *Access to Telecommunications Data in Civil Proceedings*, 27 January 2017

Coyne, Allie, 'AFP will use data retention to fight piracy', *IT News* (online), 30 October 2014 <https://www.itnews.com.au/news/afp-will-use-data-retention-to-fight-piracy-397367>

Coyne, Allie, 'Qld Police officer charged with hacking force database', *IT News* (online), 22 June 2016 <https://www.itnews.com.au/news/qld-police-officer-charged-with-hacking-force-database-421133>.

Coyne, Allie, 'AGD blind to offshore storage of Aussie metadata', *IT News* (online), 6 February 2017 <https://www.itnews.com.au/news/agd-blind-to-offshore-storage-of-aussie-metadata-451432>.

Coyne, Allie, 'Qld cop charged with misusing database', *IT News* (online), 21 March 2017 <https://www.itnews.com.au/news/qld-cop-charged-with-misusing-database-455534>

Farrell, Paul, 'Australian police accessed phone records of asylum whistleblower', *The Guardian (Australian Edition)* (online), 24 May 2016 <https://www.theguardian.com/australia-news/2016/may/24/australian-police-accessed-phone-records-of-asylum-whistleblower>

Fox, Andie, 'As a struggling single mother, Centrelink terrorised me over ex-partner's debt', *The Canberra Times* (online), 06 February 2017 <http://www.canberratimes.com.au/lifestyle/life-and-relationships/real-life/as-a-struggling-single-mother-centrelink-terrorised-me-over-expartners-debt-20170205-gu61nu.html>

Fung, Brian, 'What to expect now that Internet Providers can collect and sell your Web browser history' *The Washington Post* (online), 29 March 2017 <https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?utm_term=.d5b1538b0523>

German Working Group on Data Retention (AK Vorrat), *Criminologists: No "security gap' without blanket communications data retention* (08 February 2012) <http://www.vorratsdatenspeicherung.de/content/view/534/55/lang,en/>.

Holmes, Zeb, *Centrelink's Release of Critic's Personal Information May Be a Crime* (10 April 2017) Sydney Criminal Lawyers < http://www.sydneycriminallawyers.com.au/blog/centrelinks-release-of-critics-personal-information-may-be-a-crime/>.

Human Rights Committee, *CCPR General Comment 16: article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc HRI/GEN/1/Rev.1 (8 April 1988)

Human Rights Committee, *General Comment 12: Freedom of Movement (Art 12)*, UN Doc CCPR/C/21/Rev.1/Add.9 (18 October 1999)

Human Rights Committee, *Views: Communication No 488/1992*, 50th sess, UN Doc CCPR/C/50/D/1992 (31 March 1994)

Human Rights Council, *Special Rapporteur on Trafficking in Persons, Especially Women and Children*, 8th sess, UN Doc A/HRC/8/L.17 (12 June 2008)

Human Rights Council, *Special Rapporteur on Trafficking in Persons, Especially Women and Children*, 8th sess, UN Doc A/HRC/RES/8/12 (18 June 2008)

Johnston, Rae, 'NBN Investigation: Australian Federal Police to Raid Parliament Again', *Gizmodo* (online), 24 August 2016 <https://www.gizmodo.com.au/2016/08/nbn-investigation-the-australian-federal-police-to-raid-parliament-again/>

Knaus, Christopher and Paul Farrell, 'Centrelink recipient's data released by department to counter public criticism', *The Guardian (Australian Edition)* (online), 27 February 2017 <https://www.theguardian.com/australia-news/2017/feb/27/centrelink-recipients-data-released-by-department-to-counter-public-criticism>

La Rue, Frank, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17th sess, Agenda item 3, UN Doc AHRC/17/27 (16 May 2011)

McIlroy, Tom, Fergus Hunter and Rania Spooner, 'Red Cross data leak: personal data of 550,000 blood donors made public', *The Sydney Morning Herald* (online), 28 October 2016 <http://www.smh.com.au/federal-politics/political-news/red-cross-data-leak-personal-data-of-550000-blood-donors-made-public-20161028-gscwms.html>

Macaskill, Ewen, and Gabriel Dance, 'NSA Files: Decoded. What the revelations mean for you', *The Guardian (The Australian Edition)* (online), 01 November 2013 <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

Macquarie Dictionary Online. *Privacy* (August 2016) Pan MacMillian Australia <https://www-macquariedictionary-com-au.simsrad.net.ocs.mq.edu.au/features/word/search/?word=privacy&search_word_type=Dictionary>

Malone, Paul, 'Centrelink is an easy target for complaints but there are two sides to every story', *Sydney Morning Herald* (online), 26 February 2016 <http://www.smh.com.au/comment/centrelink-is-an-easy-target-for-complaints-but-there-are-two-sides-to-every-story-20170224-gukr4x.html>

Mills, Tammy, 'Police officer charged with unauthorized access to LEAP database', *The Age* (online), 20 may 2015 <http://www.theage.com.au/victoria/police-officer-charged-with-unauthorised-access-of-leap-database-20150520-gh5tzj.html>

'Minister referred to police over release of Centrelink details', *The New Daily* (online), 02 March 2017 <http://thenewdaily.com.au/news/national/2017/03/02/minister-referred-police-release-centrelink-details/>

Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014)

Oxford English Dictionary Online, *Privacy* (March 2016) Oxford University Press <http://www.oed.com/view/Entry/151596?redirectedFrom=privacy>

Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into Financial Related Crime* (2015)

Pillay, Navi, 'Right to Privacy in the Digital Age' (Speech delivered at the Expert Seminar of the UN Human Rights Council, Palais des Nations, Geneva, 24 February 2014)

Purtill, James, 'How pre-teens using metadata found a whistleblower in two hours', *ABC News* (online), 12 December 2016 <http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whisteblower-using-metadata/8113668>

Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth)

Sheinin, Martin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, 14th sess, Agenda Item 3, UN Doc A/HRC/14/46 (17 May 2010)

Solon, Olivia, 'Your browsing history may be up for sale soon. Here's what you need to know', *The Guardian (Australian Edition)* (online), 28 March 2017 <https://www.theguardian.com/technology/2017/mar/28/internet-service-providers-sell-browsing-history-house-vote>.

Sveen, Benjamin, 'Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted', *ABC News* (online), 04 October 2016 <http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648>.

The Right to Privacy in the Digital Age, GA Res 68/167, UN GAOR, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (18 December 2013)

Towell, Noel, 'Busted: Australian Taxation office exposed voter-profiling its own public servants during industrial ballot', *The Canberra Times* (online), 14 March 2017 <http://www.canberratimes.com.au/national/public-service/busted-public-services-voter-profiling-exposed-20170310-guv8uy.html>.

United States Congress Select Committee, *Intelligence Activities and the Rights of Americans, Book II: Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Congress (1976)

Watson, Libby, 'US Congress Just Gave Internet Providers The Green Light To Sell Customers' Browsing History Without Consent', *Gizmodo* (online), 29 March 2017 <https://www.gizmodo.com.au/2017/03/us-congress-just-gave-internet-providers-the-green-light-to-sell-customers-browsing-history-without-consent/>

Watts, David, Victorian Commissioner for Privacy and Data Protection, Submission to the Attorney-General's Department, Parliament of Australia, *Access to Telecommunications Data in Civil Proceedings*, 27 January 2017

Wheeler, Tom, 'How the Republicans Sold Your Privacy to Internet Providers', *The New York Times* (online), 29 March 2017 <https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html?_r=0>

ANNEXURE A: HISTORY OF PRIVACY PROTECTION IN AUSTRALIA

Unlike the experience of some other former British colonies, Australia does not offer rights' protections by way of a Bill or Charter of Rights. Instead, Australia has several rights and freedoms expressly stated in or implied into the Australian Constitution, while a number of other rights are protected by legislation or case law.[354] The question of privacy protection was first put before the Australian Courts in 1937 in the case of *Victoria Park Racing*.[355] While the first wave of privacy protection was being discussed and developed in the United States,[356] the majority of the Australian High Court in *Victoria Park Racing* rejected a claim of a breach of privacy as occasioned by the broadcasting of horse races from a neighbouring property.[357] At the time, Australian law and legal development followed English law closely and, as noted by Dixon J, the Court had little leeway in attempting legal innovation akin to that happening in the United States at the time.[358]

The precedent of *Victoria Park* Racing continued to be authoritative until the case of *Australian Broadcasting Corporation v Lenah Game Meats*.[359] The Court in *Lenah Game Meats* considered the precedent set by *Victoria Park Racing* and decided that the case was not about privacy but was rather about the right to control how information is made public.[360] In fact, the Court pointed out that while Australian courts have not yet developed an enforceable right to privacy, *Victoria Park Racing* 'does not stand in the path of development of such a cause of action'.[361] However, the Court in *Lenah Game Meats* refused to identify the specific elements that would form part of a common law tort of invasion of privacy, leaving the question open.

Since the decision in *Lenah Game Meats*, several privacy-related cases have been decided in various State courts in Australia, with varying interpretations of the precedent set in *Lenah Game Meats*. In 2003, the case of *Grosse v Purvis* in the Queensland District Court[362] considered the High Court decision and found that *Lenah Game Meats* rejected the position that there was no enforceable right to privacy,[363] and indeed, that an actionable civil right for damages for breach of privacy is a 'logical

---

[354] The express rights include: right to vote (s 41), right to reasonable compensation where the Crown acquires a person's property (s 51xxxi), right to trial by jury (s 80), freedom of religion (s 116), and the right of citizens of States not to be discriminated against by governments of other States (s 117); the freedom of political communication has been implied into the Australian Constitution by way of a High Court decision in *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1.

[355] *Victoria Park Racing and Recreation Grounds Company Limited v Taylor* (1937) 58 CLR 479 ('*Victoria Park Racing*').

[356] See, eg: *International News Service v Associated Press*, 248 US 215 (1918) as noted in *Victoria Park Racing* at page 509 by Dixon J.

[357] *Victoria Park Racing* (1937) 58 CLR 479 per Latham CJ, Dixon and McTiernan JJ (Rich and Evatt JJ dissenting).

[358] Ibid 496.

[359] (2001) 208 CLR 199 ('*Lenah Game Meats*').

[360] Daniel Stewart, 'Protecting Privacy, Property and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd' (2002) 30(1) *Federal Law Review* 177, 177.

[361] *Lenah Game Meats* (2001) 208 CLR 199, 248-249.

[362] [2003] QDC 151 (16 June 2003).

[363] Ibid [424].

and desirable step'.[364] Further, in *Jane Doe v Australian Broadcasting Corporation*, the Victorian County Court awarded a rape victim compensation when her name was published in contravention of court Order.[365] In this case, Her Honour considered that the Court was entitled to follow the pathway of *Lenah Game Meats* and *Grosse v Purvis* and that the decision in *Procopets* in 2004 was not an impediment to a finding of a breach of the right to privacy. In that case, the Court found that the law was not sufficiently developed so as to found a cause of action in breach of privacy.[366] On hearing the appeal to that decision, the Victorian Court of Appeal sided with the Court in the first instance, noting that 'the existence of a generalised tort of unjustified invasion of privacy has not been recognised by any superior court of record in Australia'.[367]

Finally, in the case of *DPP v Kaba* heard before the Victorian Supreme Court, His Honour examined previous cases dealing with the issue of unjustified intrusion into the private lives of individuals and followed the reasoning established in *Procopets* in noting that the existence of a positive right to privacy that is enforceable at common law is, at best, uncertain.[368] His Honour considered the statement of Warren CJ in the case of *WBM v Chief Commissioner of Police (Vic)*, stating that 'the question of whether such a right exists at common law, and if so, its scope, is yet to be settled by the High Court or a superior court of record'.[369] However, His Honour went on to note that despite this, there are instances recognised at common law where privacy is protected for particular purposes. In this case, His Honour stated that the principle of legality requires the court 'to consider the common law right to privacy when interpreting legislation'.[370] His Honour then went on to refer to the case of *Entick v Carrington*, stating that 'positive lawful authority was required for any state intrusion into the privacy of a person's property or person'.[371] In this sense, the Court considered the common law right to privacy of an individual against the government to be established, unless the principle of legality provides for lawful intrusions. In Australia, privacy protection at the Federal level has been largely legislated under the *Privacy Act 1988* (Cth), including the framework of the Australian Privacy Principles. For the purposes of this dissertation, the author will not conduct an examination of the overarching framework provided by the *Privacy Act 1988* (Cth), but rather will focus on the particular problems posed by mandatory metadata retention. Insofar as relevant, the *Privacy Act 1988* (Cth) interacts with the metadata retention legislation whereby metadata constitutes personal information under the *Privacy Act 1988* (Cth), though what is clear from Australia's approach to privacy

[364] Ibid [442].
[365] *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281 (03 April 2007).
[366] *Giller v Procopets* [2004] VSC 113 (07 April 2004) [169], [188] ('*Procopets*').
[367] *Giller v Procopets* (2008) 24 VR 1, 35 per Ashley JA.
[368] *DPP v Kaba* (2014) 44 VR 526, 552.
[369] Ibid.
[370] Ibid 553.
[371] *Entick v Carrington* (1795) 95 ER 807, 817-818.

protection, is that privacy interest, however manifest under common law, may be burdened by express intention of Parliament by way of legislation.

ANNEXURE B: EXTRACT FROM SECTION 187AA(1) OF THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979* (CTH)

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device.
2	The source of a communication	Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
3	The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
5	The type of a communication or of a relevant service	The following: (a) the type of communication;

Kinds of information to be kept		
Item	**Topic** **Column 1**	**Description of information** **Column 2**
	used in connection with a communication	Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6	The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.