THE UNIVERSITY OF SYDNEY

THE LEGAL AND ETHICAL IMPLICATIONS OF ELECTRONIC PATIENT HEALTH RECORDS AND E-HEALTH ON AUSTRALIAN PRIVACY AND CONFIDENTIALITY LAW

JULIE ANNE ZETLER

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF S.J.D.

FACULTY OF LAW

UNIVERSITY OF SYDNEY

8 MAY 2015

Dedication

I dedicate this work to my husband, Ivor, my daughters, Jessica and Emma, my mother, Patricia and my mother-in-law Freda who never lost faith in me.

ABSTRACT

This thesis addresses the legal and ethical issues posed by introduction of electronic patient health records. Against the background of an analysis of broader conceptual and theoretical understandings of development of electronic patient health records (EPR) and e-health regimes in Australia and comparable countries over the last few decades, the thesis critically examines the extent to which its implementation is consistent with established legal and ethical principles underpinning traditional health assumptions and practices. To this end the thesis explores the evolution and progress of modern health, technology, law and governance issues in e-health, identifying critical features of emerging EPR and e-health systems such as broad innovative industry technology involvement, and potentially problematic practices such as personal information 'collection', 'sharing' and 'networking' activities. The thesis contends that while adopting technology such as e-health comports with modern day progress, the transformational power of technology on society and individual lives has the potential to impose significant human costs for health consumers and everyday life. Through an analysis of the new electronic regime the thesis reveals how Australian Governments, healthcare providers, consumers and other stakeholders interpret and deal with advances in personal healthcare information changes in the new electronic system.

The healthcare privacy model advanced in the thesis, in conjunction with an analysis grounded in theories of deliberative democracy, provides the foundation for the thesis argument that the legal, ethical and democratic challenges posed to privacy and participation interests by implementation of e-health policies can best be alleviated in Australia through further structural reforms beyond those recently proposed by a federal review. The thesis contends that an independent 'Council', with broad powers to consult and engage the public is an important part of the solution to the political and economic problems identified by the thesis analysis showing that individual privacy protection in

healthcare is threatened and that earlier privacy protection mechanisms may prove inadequate in the emerging global information era.

Acknowledgement

This thesis represents a long (and often arduous) journey over many years and it is acknowledged that many people have encouraged and supported me throughout this voyage. It goes without saying that I am very grateful for all their assistance. I wish to especially acknowledge my supervisors: Belinda Bennett for all her time, effort and feedback; Terry Carney for his continuing encouragement, generosity of time, dedication and guidance, and Ghena Krayem, whose continuing encouraging feedback and positive disposition was very much appreciated. They all gave unstintingly of their time and expertise and without their guidance I would not be at this point.

I would also like to thank all my family and friends, particularly my mum, my sisters and niece for all their help and support that they gave to me during, at times, a frustrating and seemingly unending process of research, writing, editing and rewriting. A special thanks to my good friend and mentor Robin who read everything I wrote and provided me with encouragement and valuable feedback. Most of all I wish to thank my special family: Ivor, Jessica and Emma, for supporting me through this long process, during all the family 'dramas' over the years and being understanding when I was always at work or on my computer and unable to do the things that families really should do such as go on weekend outings.

Declaration of Originality

I hereby certify that this thesis is entirely my own work and that any material written by others has been acknowledged in the text

The thesis has not been presented for a degree or any other purposes at The University of Sydney or at any other university or institution.

In accordance with the *Thesis and Examination of Higher Degrees by Research Policy* 2015 and *Thesis and Examination of Higher Degrees by Research Procedures* 2015 that (1) no human ethics approval was required or obtained for this thesis (2) the sources which the information in the thesis is derived and (3) the nature of collaborations, or assistance, with the work described in the thesis, including (a) assistance provided during the research phase was my own and (b) only limited editorial and proof-reading assistance in writing the thesis was provided in the early stages by Joan Rosenthal and in the final stages by Renee Stevens.

The law identified in this thesis is up date as to the end of April 2015. It is acknowledged that the federal Government will release a new federal *Budget* sometime in May and that this may include adopting the Personally Controlled Electronic Health Records December 2013 *Royle Review* recommendations. The thesis is submitted before the release of the new federal *Budget*.

Table of Contents

CHAPTER 1

THESIS PROBLEM QUESTION AND BACKGROUND

The thesis inquiry traces the development and implementation of the new electronic health regime by the Australian Government. It does this by exploring the historical and theoretical progress of Electronic Patient Records (*EPR* or *PCEHR)* and e-health systems in Australia that commits to broad innovative industry technology involvement and practices including concepts such as personal health information 'collection', 'sharing', 'networking' and 'linkage' activities.[1] Changes in how Australian Governments, consumers, healthcare providers and other stakeholders interpret and deal with *EPR* and e-health has significantly impacted on established legal and ethical principles underpinning traditional assumptions and practices within health. These particular technological changes include: patient medical records — creation, collection, access, storage, control, and ownership issues, as well as individual versus collective privacy protection considerations, especially within the new expanding electronic healthcare 'sharing' environment.[2]

---

[1] Australian Health Information Council (AHIC), *E-Health Future Directions Briefing Paper* (4 October 2007); National E-Health Transition Authority (NEHTA), *Privacy Blueprint for the Individual Electronic Health Record* (3 July 2008); Australian Government, NEHTA, *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* (September 2011).

[2] Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law*: *International and Comparative Perspectives* (Cambridge University Press, 2006); Moira Paterson, *Freedom of Information and Privacy in Australia* (LexisNexis, 2005).

The central thesis proposition advances the notion that individual privacy is under threat and is in danger of being further compromised and eroded by broader economic 'networking' interests, unless there is an assurance by the Australian Government that individual privacy rights are afforded ongoing appropriate protection.[3] In order to advance the proposition that individual privacy protection is indeed compromised by the advancement of modern information technology the thesis analysis reconnoitres the growing interaction, interrelation and developing 'links' between health, technology, law and governance mechanism and its impact on communities. The privacy problem question also considers the adequacy of individual healthcare privacy protection rights in light of the transformational political, economic and social changes to Australian healthcare systems, which include recent Government policies that further extend the possibility of increasing private sector actor involvement in healthcare services, public sector and service delivery cuts, devolution policy adoption, and the future impact associated with privatisation and commercialisation of health on Australian citizens.[4]

In Western democracy, a dominate focus and preoccupation for many governments and citizens has been on recognising and promoting privacy and privacy rights. However, broader influences that extend beyond the notion of citizen privacy rights and protection have resulted in questions concerning the ongoing relevance and

[3] See Evgeny Molozov, *The Net Delusion: The Dark Side of Internet Freedom* (Penguin Books, 2011); Evgeny Morozov, "The Real Privacy Problem" (22 October, 2013) 116(6) *MIT Technology Review* 32-43.
[4] See Paul Smith, 'Battle Won, But War Not Over: Short Consult Breakdown Can't Mask Uncertain Future' *Australian Doctor* (Australia), 23 January 2015, 1 [Where Federal Health Minister, Sussan Ley, explains Government's back down regarding plans to slash Medicare funding for General Practitioner's (GP) care].

importance of privacy as a core human value in the new technology-driven world.[5] This traditional preoccupation with privacy and privacy rights is no less significant in Australia than other countries and can be evidenced over the last few decades by successive Australian Governments (and Opposition parties) backing the introduction of e-health systems, including a new electronic healthcare record regime. This e-health government policy development has generally been in response to emerging complex national and international social and economic problems.[6] Other local, national and international influences also challenging traditional healthcare delivery modalities include: an ageing population with fewer and more dispersed family support networks, increasing healthcare provision costs, remote and indigenous healthcare access and equity issues, increasing migration and cultural diversity, diminishing national, local employment opportunities and expanding globalisation.[7]

While it can be contended that adopting technology such as e-health comports with modern-day human progress, it can also be posited that there is a significant human cost in relying on technology as the determinant to everyday problems due to the danger of underestimating the transformational power that technology has on

---

[5] See, e.g. Daniel Solove, Marc Rotenberg and Paul Schwartz, *Privacy, Information and Technology* (Aspen Publishers, 2006); Daniel Solove, *The Digital Person* (New York University Press, 2004); Jeffrey Rosen, *The Unwanted Gaze* (Vintage Books, 2000); see also National E-Health and Information Principal Committee, Deloitte, *National E-Health Strategy* (30 September, 2008): at 8-10.

[6] See House of Representatives Standing Committee on Family and Community Affairs, *Health on Line* (1997); see also John Mitchell, National Office for the Information Economy, Department of Communication, *From Telehealth to E-Health: The Unstoppable Rise of E-Health* (1999)

[7] See Stephen Sammut, 'Biotechnology Business and Revenue Models: The Dynamic of Technological Evolution and Capital Market Ingenuity' in Lawton Robert Burns (ed), *The Business of Healthcare Innovation* (Cambridge University Press, 2005): at 190; Deloitte, *National E-Health Strategy*, above n5; George Palmer and Stephanie Short, *Health Care and Public Policy* (Palgrave Macmillan, 4th ed, 2010): at 38; Sandra Taylor, Michele Foster and Jennifier Fleming (eds), *Health Care Practice in Australia* (Oxford University Press, 2008); Eileen Willis, Louise Reynolds and Helen Keleher (eds), *Understanding the Australian Health Care System* (Elsevier, 2012); Smith, Paul, 'Will Universal Healthcare Survive the MBS Ice Age?' *Australian Doctor* (Australia), 3 April 2015, 3.

society and individual lives.[8] For all the above reasons the thesis contends that it is now imperative for Australians to recognise that individual healthcare privacy rights are under threat by advancing reliance on modern technology and begin to question healthcare privacy protection rights in light of these political, economic and social changes.[9] Given this consideration, the thesis maintains that one significant way to begin the process of raising citizen awareness and involvement in protecting healthcare privacy rights is to shift the focus away from advancing capitalist economic imperatives and back on what local society and individuals expect from a modern participatory democracy.[10]

The thesis asserts that broader social, political and economic 'macro' concerns, as well as 'micro' changes now underpin our concept of health and that these changes impact upon individual healthcare privacy rights in the modern information economy era. To demonstrate the extent of the problem facing individual healthcare privacy protection, the thesis exploration captures relevant theoretical concepts, legal and ethical obligations, along with possible solutions that aim at supporting, supplementing and strengthening individual privacy protection in Australia.

I. AN INDEPENDENT COUNCIL FOR AUSTRALIA

---

[8] See Simon Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001) 143; see also Christopher Arup, *Innovation, Policy and Law: Australia and the International High Technology Economy* (Cambridge University Press, 1993).

[9] See, e.g. Philip Allott, *The Health of Nations: Society and Law Beyond the State: Society and Law Beyond the State* (Cambridge University Press, 2002); Lawton Robert Burns (ed), *The Business of Healthcare Innovation,* above n5; Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011).

[10] See chapter 2, pp41-42

The thesis develops an argument for proposed privacy protection solutions that would strengthen individual privacy rights, ensure cross-government coordination, accountability and further support existing public participation mechanisms for the implementation of *PCEHR* and e-health systems include: fixing legal fragmentation caused by harmonising privacy legislation; ensure local democratic citizen participation in the new *PCEHR* system, and insisting upon better long-term transparent management of e-health privacy technical measures and processes. The thesis argues that an important step towards realising some of these goals would be by introducing an *Independent Council* (*'Council'*). It is envisaged that this would guarantee citizen visibility, encourage wider participation and foster much needed consumer and healthcare provider confidence and voluntary uptake of the *PCEHR* and e-health system;[11] as well as insist upon Government and non-government action transparency and open government measures in light of advancing healthcare privatisation and commercialisation adoption.

The creation, purpose, character, formation, membership, details and function of a *Council* are the subject of detailed discussion in light of the thesis analysis of the issues and concerns raised by *EPR* and e-health.[12] However, it is anticipated that the membership of a *Council* would include a broad range of citizen representatives from across Australia[13] — with wide powers to conduct hearings, access and disseminate

[11] See John Dryzek and Patrick Dunleavy, *Theories of the Democratic State* (Palgrave Macmillan, 2009); see also John Braithwaite, *Regulatory Capitalism* (Edward Elgar, 2008); Philip Allott, *The Health of Nations,* above n9; Andrew Kenyon, et al, *New Dimensions in Privacy Law: International and Comparative Perspectives*, above n2.

[12] See chapter 6, pp184-187; chapter 7, pp255-260.

[13] See chapter 7 for details for the proposed structural mechanisms and membership of a *Council,* pp255-260.

information, and liaise with appropriate governing and coordinating bodies[14] ensuring that it can discharge its responsibility for identifying and reporting to the public, independently of Parliament and Ministers, on the likely impact of administrative policy decisions relating to current and future *PCEHR*, e-health implementation and roll-out systems.

The thesis analysis is predicated on the recognition that healthcare issues are multifarious and that there is an urgent need to find appropriate solutions to complex dilemmas relating to values and concepts attached to civil liberties and human rights,[15] and that this involves consideration of the advancement of modern-day commercial reality that insists upon the notion of competition and 'free flow' information markets.[16] The ensuing tension between humanisation and commodification processes is not unique to healthcare and remains a major concern for all aspects of modern day social intercourse including employment and welfare.[17] To help counterbalance the very real problem of government's adoption of market competition ideology and the power of technology to transform citizen healthcare

---

[14] See Panel members, Richard Royle, Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013). A recommendation proposed by the *Royle Review*, included the establishment of an Australian Commission for Electronic Health ('*ACeH*') and the Standing Council on Health ('*SCoH*'): at 10.

[15] Richard Stone, *Civil Liberties & Human Rights* (Oxford University Press, 7th ed, 2008); Lawton Robert Burns (ed), *The Business of Healthcare Innovation*, above n7.

[16] See Subramanian and Katz, *The Global Flow of Information*, above n9; see also Brian Galligan, Winsome Roberts and Gabriella Trifiletti, *Australians and Globalisation: The Experience of Two Centuries* (Cambridge University Press, 2001); see also Rhacel Salazar Parrenas, *Servants of Globalisation: Women, Migration and Domestic Work* (Stanford University Press, 2001).

[17] See Martha Nussbaum, 'Educating Citizens' in Martha Nussbaum, *Not for Profit: Why Democracy Needs the Humanities* (Princeton University Press, 2010): at 27; Huw Beverely-Smith, *The Commercial Appropriation of Personality* (Cambridge University Press, 2008); Frederick Lane, *The Naked Employee* (Amacom, 2003); Peter Jackson, Michelle Lowe, Daniel Miller and Frank Mort, *Commercial Cultures* (Berg Publication, 2000); Robert Locke and J-C Spender, *Confronting Managerialism* (Zed Books, 2011); Dexter Dunphy, Andrew Griffiths and Suzanne Benn, *Organisational Change for Corporate Sustainability* (Routledge Press, 2003).

recipients into passive receivers of goods and services,[18] it is proposed that mechanisms be introduced to further strengthen democratic processes and supplement citizen healthcare privacy protection such as through the *Council* advanced in the thesis. In other words the purpose of a *Council* is to primarily focus on the local/national citizen interests rather than international impact of electronic privacy reform.

Given the thesis focus on Australian health, technology, governance and privacy concerns, chapter 2 begins this e-health analysis by tracing historical and evolving health development government policy trends over the last few decades in Australia. Furthermore the chapter identifies the multiple dimensions that help delineate contextual understanding of modern-day Australian health, privacy and technology concerns. This exploration provides a 'framework' for understanding the political, economic and social influences that underpin how health, privacy and technology are connected and why this area of human activity remains an important concern for ongoing Australian citizen involvement.

Additionally, it is argued that there is a major shift by the current federal Coalition Liberal Government away from its primary responsibility of providing healthcare delivery and maintaining leadership within health, to that of political economic 'enabler', whose main purpose is to serve the expanding needs of a growing number of private/public economic actors who wish to invest and engage in healthcare delivery opportunities. This recent political change is shown to be important to Australian healthcare delivery systems because it has the potential to

[18] Evengy Morozov, "The Real Privacy Probem", above n2: at 3

transform the focus and overall outcome of healthcare provision (and privacy protection rights) in Australia away from established administrative law values such as transparency and accountability towards private sector economic imperative principles such as 'commercial in confidence' and 'competitive business needs' and values, potentially altering the very nature of what have previously been understood as healthcare rights in this country.[19]

Chapter 3 continues the health, technology and privacy focus analyses by detailing the nature and scale of the challenges to privacy and democratic policy-making posed by the technologies implicated in an electronic healthcare regime. It provides a deeper conceptual analysis of the evolution of technology and the transformational power of technology on society and highlights various concerns about electronic healthcare privacy. Appreciating how technology has impacted on not just health in Australia but other significant aspects of day-to-day life contributes to a fuller awareness of the awesome transformational power of technology in reconceptualising clinical, social and legal issues. Specifically, this chapter argues that e-health technology gives rise to an increasingly 'symbiotic' relationship between health and technology: one which is more multi-faceted, more interconnected (linked),

[19] See Moira Paterson, *Freedom of Information and Privacy in Australia*(LexisNexis, 2005); see also 'Royle Review', above n14; see also Andreas Georg Scherer and Guido Palazzo, "The New Political Role of Business in a Globalised World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy" (4 June 2011) 4 *Journal of Management Studies* 48; Pat Barrett, Auditor-General for Australia, 'Public Private Partnerships – Are There Gaps in Public Sector Accountability?' (Paper Presented at 2002 Australasian Council of Public Accounts Committees 7th Biennial Conference, Melbourne, 3 February 2003). 'This paper considers the question of public sector accountability in the context of public-private partnerships (PPPs) for the delivery of public sector outcomes; and the challenges facing Parliaments in protecting the public interest and maintaining accountability for the expenditure of public funds': at 1; Colin Fisher and Alan Lovell, *Business Ethics and Values* (Prentice Hall, 3rd ed, 2009); Marvin Brown, *Corporate Integrity: Rethinking Organisational Ethics and Leadership* (Cambridge University Press, 2005).

and more 'complex' than was the case with the technologies replaced; one that chapter 4 will suggest has implications in terms of calling forth a need for more complex or relational concepts of privacy to mirror these characteristics. To this end, chapter 3 identifies and discusses the legal and ethical responses to modern technology including those associated with healthcare, referred to by Ronda Jolly as a 'revolution' in health.[20] Furthermore, chapter 3 highlights a very significant aspect of the healthcare privacy debate, which is the way e-health technologies necessarily interface with the threats to privacy generated by the rapid development of national and international surveillance, security and biometric mechanisms since the 'war on terror'.[21]

To progress the thesis argument that electronic healthcare privacy rights requires further consideration and protection in our modern technology driven age, chapter 4 presents what the thesis contends is the appropriate conceptual understanding of the notion of privacy. This chapter reviews key contours of the debate surrounding different concepts of privacy whilst arguing in favour of a particular theoretical framework of privacy, which best captures the challenges posed by the 'symbiotic' relationship between health and technology. Chapter 4 argues that such a relational conception of privacy requires renewed consideration by governments and public sector decision-makers of what may be termed public law

[20] See Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done' (Research Paper No 3, Parliamentary Library, Parliament of Australia, 17 November 2011).

[21] See Helen Duffy, *The 'War on Terror' and the Framework of International Law* (Cambridge University Press, 2005). According to Duffy the term 'war on terror' was first used by George W Bush (US President) on 20 September 2001: at 2.

elements or mechanisms, such as by incorporating into healthcare privacy protection administrative law values and principles such as transparency and accountability.[22]

Chapters 2, 3 and 4 do not suggest that the Australian Government has not been transparent in its dealings relating to individual privacy protection in the past (existing avenues for healthcare policy feedback have been acted upon in a transparent and accountable fashion). Rather, these chapters provide a basis for the thesis contention that there is considerable room to supplement these existing mechanisms, and that the adoption of a *Council* would promote the notion of citizen participation, accountability and transparency further.

Chapter 5 provides an analysis of the current legal arguments concerning health and privacy regulations and highlights the shortcomings of common law and statutory law in protecting individual privacy rights and the numerous challenges posed by ongoing legal fragmentation that exists in Australia when it comes to health and privacy regulations. It also emphasises the inconsistent approaches and problems associated with federalism such as federal, state and territory responses to health and privacy and the impact this has on the present situation. It does this by recognising constitutional limitations existing in the area and the effect this has on a uniform 'harmonised' approach to the broader problems and challenges of privacy protection.[23] The chapter provides an outline of the relevant states/territory and

[22] See Pat Barrett, Auditor-General for Australia, 'Public Private Partnerships – Are There Gaps in Public Sector Accountability?' above n19; Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20.

[23] Dan Jerker B Svantesson, "Privacy, The Internet and Transborder Data Flows: An Australian Perspective" (2007) 19 Bond Law Review 1; see ALRC, *Serious Invasions of Privacy in the Digital Era*: Issues Paper 43 (October 2013).

federal response to healthcare and healthcare privacy and limitations associated with a more coordinated approach by inter-governmental bodies such as the Council of Australian Governments (COAG).

To illustrate the gravity of the challenge of legal fragmentation, the chapter analyses of privacy reports and government responses to these reviews is highlighted. For instance, in response to the Australian Law Reform Commission ('ALRC') 2008 report and recommendations in — *For Your Information: Australian Privacy Law and Practice* — and the ALRC final report in September 2014 — *Serious Invasions of Privacy in the Digital Era* — this chapter outlines recent legislation on health privacy.[24] By demonstrating the inadequacy of existing legal approaches across the federation to the problem of privacy rights and protection in light of economic and social changes, the chapter makes the case for a coordination and liaison role of the proposed *Council* in relation to the government's trilogy solution — legislation, technical measures and governance — and its first leg namely legislation.[25]

---

[24] See ALRC, *Review of Australian Privacy Law*: Discussion Paper 72 (September 2007);ALRC, *For Your Information: Australian Privacy Law and Practice*: ALRC Report 108 (August 2008); ALRC, *Review of Privacy*: Issues Paper 31 (October 2006); ALRC, *Serious Invasions of Privacy in the Digital Era*: Discussion Paper 80 (March 2014); ALRC, *Serious Invasions of Privacy in the Digital Era - Final Report*: ALRC Report 123 (3 September 2014); see also ALRC, *Copyright and the Digital Economy*: Summary Report 122 (November 2013); ALRC, Issues Paper 43, above n23.

[25] See ALRC, Issues Paper 43, above n23. Issues Paper 43 recognises 'gaps' in the existing Australian law such as that the *Privacy Act 1988* (Cth) and 'State and Territory equivalents deal only with information privacy and not with intrusions into personal privacy': at 47. It also acknowledges that there is 'no tort or civil action for harassment, nor is there sufficient deterrence against 'cyber-harassment' in Australian law, compared with overseas jurisdictions' (see, for example, Nova Scotia, Canada, *Cyber-Safety Act*, SNS 2013, c 2 criminalises cyber-bullying): at 47.

Chapter 6 considers the other two trilogy solutions proposed by the previous federal Government[26] — technical measures and *PCEHR* and e-health governance — and provides further insight into their current application and status. This chapter extends the privacy protection analysis beyond the legal dimensions by exploring other various proposals for the adoption of privacy-friendly technical and *PCEHR* governance measures. Chapter 6 also includes an analysis of earlier and recent government and other recommendations about how governance in this area should be organised.[27] This chapter adopts a multi-dimensional approach by identifying the wider political and economic shift in healthcare governance discourse and its importance in Australia's political, economic and social context.

Given the information contained and discussed in chapters 2, 3, 4, 5 and 6, chapter 7 concludes the thesis by summarising the main arguments and reinforcing the thesis proposition that a *Council* will further the objectives of strengthening individual privacy protection, accountability and coordination issues confronting the new electronic health regime. It does this by questioning and extending orthodox healthcare theories of privacy that have a tendency to limit public input in the area, as well as recognising and responding to the changing political dynamics in Australia. The chapter argues that reliance on antiquated concepts of privacy in a rapidly changing environment have a tendency to restrict the debate and the democratic

[26] See NEHTA, *Concepts of Operations*, above n1. The *Concepts of Operations* report document sets out the proposed government privacy protection trilogy as encompassing – legislation, technical measures and governance: at 20-21.

[27] See, for example, '*Royle Review*', above n14.

process.[28] Prior privacy protection machinery put in place by the Australian Government have recognised the importance of healthcare provider experts and other stakeholders such as business interests and consumer advocacy groups. However despite the creation of expert Councils and Committees, there continues to be dissatisfaction relating to the power of the expert such as health industry and professional groups to influence and direct *EPR* and e-health policy changes. This chapter examines the reasons why the current approach taken by government in regards to affecting policy change by self-interested expert groups such as medical practitioners has not worked and why a *Council* is necessary to direct and oversee changes occurring in this area.

Furthermore chapter 7 posits that while it can be appreciated that current proposed trilogy of privacy protective mechanisms — legislation, governance and technical measures — go a long way towards balancing an individual's healthcare information rights, this mechanism alone provides insufficient protection in light of growing contextual social, economic and political changes that impact on modern society. This is because existing privacy protection mechanisms do not sufficiently anticipate or reflect the rapid transformation powers of information technology and its overall effect on democracy to drive digital information data collection, use and disclosure in the new knowledge and information economy.

[28] See Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom,* above n1; see also Evgeny Morozov, "The Real Privacy Problem", above n3; see also Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008); Daniel Solove, *Nothing to Hide* (Yale University Press, 2011); Daniel Solove, *The Digital Person,* above n5; Martha Nussbaum, *Not for Profit*, above n17: at 47-77 [Nussbaum supports the notion of citizen engagement and debate such as Socratic Pedagogy and highlights the importance of argument].

II. METHODOLOGY AND THESIS CHAPTER STRUCTURE AND CONTENT

The methodology employed in the thesis represents a combination or 'mixed mode' approach and includes literature review, historical analysis, theoretical and ethical inquiry, case studies and legal critique. This combination approach to methodology will support the contextual framework of privacy, health, technology and law and progress the thesis argument by enabling exploration of both 'macro' 'meso' and 'micro' issues that arise in the inquiry. It is integral to the Australian Government approach that the adoption of information technology (IT) is a key component of communication,[29] and therefore it is incumbent that any examination of developing health technology and issues around broad privacy protection requires a solid understanding of the available government and scholarly literature in order to appreciate the extensive range of national and international information, opinions and debate in the area.

The thesis adopts historical analysis in order to contextualise and frame current understanding of privacy and privacy issues arising from health, technology, privacy and law. The relevance of utilising theoretical, ethical and legal enquiry is that it distinguishes the foundational concepts and discourse that underpin questions such as why health privacy values are important and why we need to protect privacy rights in the future. Case scenarios are also included in the analysis because they extend and

[29] See Australian Government, *National Health Reform: Progress and Delivery* (September 2011) 1.

support theory development; they do this by demonstrating, in a practical way, how health, technology, law and ethics impact on individual privacy.[30]

It is foreshadowed that identifying the evolution of Australian health law,[31] *EPR* and e-health systems will provide a deeper appreciation of the legal advantages and disadvantages (limitations) of current and proposed confidentiality and privacy protection instruments. Importantly, it will be argued that law represents a very significant regulatory mechanism for promoting individual privacy protection in the digital age and needs to take a more active role in modern-day human rights protection. Moreover the thesis acknowledges the increasing number of related legal problems such as surveillance, cybercrime, identity theft and intellectual property activities that will also impact substantially on individual privacy protection rights.[32]

To conclude, as the above chapter content summary explains, Chapters 2-7 will support the main thesis. This primary focus is achieved by providing an analysis of the introduction of the new electronic health regime by Australian Government's policy and law commitments over the last few decades and the impact this development has had on individual healthcare privacy protection in Australia. Against this background of an analysis of broader conceptual and theoretical underpinnings of development of *EPR* and e-health regimes in Australia and comparable countries over the last few decades, the thesis also attempts to critically examine the extent to which its implementation is consistent with established legal

[30] See chapter 3, pp78-79.

[31] See chapter 5, pp146-163.

[32] See chapter 5, pp163-174; chapter 3, pp78-80.

and ethical principles underpinning traditional health assumptions and practices. As a consequence of the broader comparative analysis requirement the following discussion on international *EPR* and e-health considerations and international privacy protection highlights how, similar to Australia, other countries have adopted *EPR* systems and examines what lessons Australia might take away from these international experiences. Additionally, it is contended that identifying the broader international experience and challenges of e-health implementation and its impact on privacy and democratic rights provides further confirmation of the multi-dimensional and economic complexity of this type of technology on individual lives.

III. INTERNATIONAL ELECTRONIC PATIENT RECORDS AND E-HEALTH

The formal introduction of *EPR* and e-health of course is not confined to Australia and since the 1990s the potential of e-health has been discussed globally, but remains a work in progress in most countries. Many Western countries in some parts of Europe,[33] as well as the United Kingdom (UK), Canada and New Zealand have over the last few decades introduced *EPR* and e-health systems into their healthcare delivery programs. Indeed even in 2015 *EPR* and e-health systems are well advanced in many places including Canada and New Zealand and it is recognised that Australia lags behind in its IT investment and infrastructure development in the area.[34] However, despite the availability of extensive knowledge from other countries regarding *EPR* and e-health systems implementation experiences, the thesis has

[33] See, for example, Norway, Denmark, Sweden and Germany.

[34] See Deloitte, *National E-Health Strategy*, above n5: at 21.

elected, due to the focus on Australia, to engage in an in-depth exploration of selected countries in order to highlight shared concerns relating to the introduction of *EPR* rather than provide a comprehensive analysis of international *EPR* and privacy law.

A. *Parts of Europe*

Examples of international *EPR* and e-health investment can be seen in countries such as Norway, Denmark, Germany and UK. For instance, every patient in Norway, Sweden and Denmark is allotted a unique personal identifier. Norway has achieved a remarkably high degree of *EPR* penetration with more than 90 per cent of healthcare providers using e-health technology and patient records.[35] Norway has a dedicated healthcare 'network' — the National Health Network (Health Information Technology (HIT)), which interconnects five health networks and provides a number of basic services such as web, email, catalogues and registries of personnel.[36]

In 2013-2014 despite much progress in the uptake of e-health and patient records it was recently reported that Norwegian primary care is still fragmented and in some areas of service lacks the resources and equipment for its implementation.[37] All hospitals use electronic health records, but the lack of structured patient records in both primary and secondary care precludes automatic data extraction; hence there

[35] The Commonwealth Fund, *International Profile of Health Care Systems, December 2013* (December 2013): at 90-91.

[36] See Jan Tore Lium and Arild Faxvaag 'Removal of Paper-Based Health Records From Norwegian Hospitals: Effects on Clinical Workflow' (Report Norwegian Research Centre for Electronic Patient Records, Faculty of Medicine, Norwegian University of Science and Technology, Trondheim, Norway, 2006): at 1-2.

[37] The Commonwealth Fund, *International Profile of Health Care Systems*, above n35: at 90.

is insufficient data for quality improvement or national activity registration at both the local and national level.[38]

Denmark is described as a 'shining example' and records the highest satisfaction with the healthcare system.[39] In 2008 Danish General Practitioners (GPs) were ranked first by the European Commission report on the use of health IT in Europe. In a recent 2013 report —*International Profile of Health Care Systems, December 2013* — it noted that Danish Information technology (IT) is used at all levels of the health system.[40] The primary Danish Health Care Data Network is Med*Com* and it is responsible for developing a strategy for digitisation of Denmark's healthcare service.[41]

The *Sundhed.dk* is a national IT portal for Denmark with differentiated access for health staff and the public. The portal provides general information on health and treatment options and access to individual's own medical records and history.[42] A number of factors contribute to the Danish e-health system success, including: the countries relatively small size and population (about 5 million), with an IT-savvy citizenry; trust in the federal Government is high; the countries healthcare is run by

---

[38] The Commonwealth Fund, *International Profile of Health Care Systems*, above n35; see also Robert Fichman, Rajiv Kohli and Ranjani Krishnan, "The Role of Information Systems in Healthcare: Current Research and Future Trends" (September 2011) 22 (3) *Information System Research* 419-428; D A Ludwick and John Doucette, "Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries" (2009) 78 *International Journal of Medical Informatics* 22-31

[39] Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20: at 7.

[40] See The Commonwealth Fund, *International Profiles of Health Care Systems, 2013,* above n35; National Board of Health, Denmark, *National Strategy for Information Technology in the Health Care System,* (2003-2007) published 2002. Sets out shared EPR concept models including security and patient rights, multidisciplinary operation and common national terminology: at 6-7.

[41] Med*Com Denmark E-Health and Implementation of EHR* Hall in Tirol 26.04.2006 http://www.ehealth-benchmarking.org/2006/images/stories/06-johansen_denmark.pdf (viewed on 16/6/2012).

[42] The Commonwealth Fund, *International Profiles of Health Care Systems, 2013,* above n35: at 30.

the public sector, and the Danish Government placed a high priority on engaging GPs. The Government also provided and paid for technical support for primary care practitioners to encourage widespread adoption of electronic records.[43]

In contrast to Norway and Denmark, the German healthcare system is the biggest in Europe. Germany has a detailed specification of its technical and organisational framework for IT including information, communication, healthcare privacy and security, providing the basis for the introduction of its national smartcard.[44] In 2013, it was estimated that approximately 90 per cent of physicians in private practice use *EPR* to help with billing, documentation, tracking laboratory data and quality assurance. In some regions about 60 per cent of physicians use online services to transmit information. In Germany a unique patient identifier does not exist as data-safety concerns still represent a significant obstacle for its introduction.[45] For example, the German medical profession continues to express fears that *EPR* and e-health implementation will result in the loss of privacy, increase security risks associated with electronic prescriptions, bringing an increased reliance on digital signatures, as well as the increasing threat of bureaucracy and government oversight to professional independence.[46] Similar to current 2015 Australian GP pleas for reimbursement of costs, German doctors also sought the provision of *EPR* payment and reimbursement of costs for technology set-up and professional time. This battle

[43] K Stroetmann, J Artmann, V Stroetmann with D Protti, J Dumortier, S Giest, U Walossek and D Whitehouse, 'European Countries on Their Journey Towards National E-Health Infrastructures: Final European Progress Report ICT for Health Unit', European Commission, January 2011 cited in Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20: at 6-7.

[44] Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20.

[45] E-Health ERA, *E-Health Strategy and Implementation in Germany* (30 June 2007).

[46] E-Health ERA, *E-Health Strategy*, above n45.

for *EPR* reimbursement and compensation remains an open-ended issue in Germany.[47]

Apart from the ongoing professional issues, the greatest problem with implementing a system wide *EPR* in Germany is the continuing incompatibility of the different programs within and between hospitals, and between hospitals and ambulatory care. Previously, Germany implemented an earlier version of an electronic medical chip card (KVK), however, on 1 January 2015, this card, which is universal, has now been replaced — by the 'elektronische Gesundheitskarte' (electronic health card).[48] The 'Gesundheitskarte' is issued to citizens by statutory health insurance providers and gives doctors and dentists access to patient data via an electronic chip located on the card.[49] The new electronic health card can only be used for health treatment; to further ensure privacy the health card is also available with or without an identity photograph on the card.

E-health and *EPR* progress in the United Kingdom (UK) illustrates a number of difficulties that can be encountered in realising e-health initiatives. The implementation of a Personal Demographic Service (PDS), which comprises demographic information such as name, address, date of birth and National Health Service (NHS) number, commenced across the UK in July 2004. Despite holding no clinical health information the PDS has long been considered the first step towards instigating *EPR* for every patient registered with the NHS and replacing NHS regional

[47] See Sarah Colyer, 'E-health Indemnity Stand-off' *Australian Doctor* (Australia), 15 June 2012, 1; Paul Smith, 'Big Stick Looms Over e-Health' *Australian Doctor* (Australia), 18 May 2012, 3.

[48] E-Health Europe, *Germany's National e-Health Programme: Contested but Driven Forward* (17 June 2012).

[49] E-Health Europe, *Germany's National e-Health Programme*, above n48: at 1.

databases.[50] Authorised healthcare professionals are able to access the PDS through a health smartcard.[51] Every patient registered with the NHS receives an NHS number, which acts as a unique patient identifier. Most GP patient records are computerised. Some practices use electronic systems to allow patients to make appointments and e-mail their GP but there is no requirement to do so. However, hospitals and general practice records are not integrated into a single system.

In the UK the previous Labour Government attempted to introduce a patient record covering all service providers, but due to circumstances at the time had to abandon it because of cost and other factors. For example, in 2007 the House of Commons Committee of Public Accounts in its first report — *National Programme for IT in the NHS: Twentieth Report of Session 2006-2007* ('*First Report*')—questioned the enormous costs and limited benefits derived from the National Health IT Program.[52] The *First Report* considered the current status of shared electronic patient clinical records, the costs of the program, the local management and implementation of the system within the NHS, the extent of clinician involvement, and patient confidentiality and security risks.[53] The *First Report* noted the high stakes of the IT Program and acknowledged that electronic technology could revolutionise the way

---

[50] Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20: at 10.

[51] See also UK, National Health Services (NHS), *Connecting for Health 'Spine'* (2012). UK Government pushed its implementation of a national EPR and e-health vision forward by creating the 'SPINE' Program. This program remains one of the largest civilian projects in the world and operates 24 hours a day, 365 days a year to provide the IT infrastructure and support programs for GPs and Pharmacists in the UK, including the Summary Care Record, electronic prescription service connections, NHS number and secondary use services.

[52] UK Parliament, Comptroller and Auditor General (C&AGs) Report, *Department of Health: The National Programme for IT in the NHS, HC* (2005-2006) (March 2006): at 1173.

[53] UK Parliament, House of Commons Committee of Public Accounts, *Department of Health: The National Programme for IT in the NHS' Twentieth Report of Session 2006-2007* (26 March 2007) ('*First Report*'): at 1.

the NHS in the UK used information, including patient healthcare information. However, it was equally observed by the report that if it failed it could set back IT developments in the NHS for years and divert money and staff time from frontline patient services.[54]

The *First Report* recommendations formed the basis for the later 2011 House of Commons Committee of Public Accounting —*The National Programme for IT in the NHS: An Update on the Delivery of Detailed Care Records Systems* (*'Second Report'*) —of healthcare record systems in the UK.[55] The *Second Report* found that the implementation of an alternative up-to-date IT system had once again significantly fallen behind schedule and costs had continued to escalate.[56] Further it was noted that the Department of Health had now accepted its inability to deliver its original vision of a standardised care record system for NHS patients and as a result was now relying on individual NHS Trusts to develop systems compatible with those in the program. This situation indicated that different parts of the country continued to rely on dissimilar systems that might be incompatible with each other. It was also recommended that the Department review its commitment to the program and consider whether the remaining £4.3 billion would be better spent elsewhere. In its findings the *Second Report* was very critical of the fact that the Department of Health had not received the best out of suppliers, despite having paid them some £1.8 billion

[54] UK Parliament, *First Report*, above n53.

[55] UK Parliament, House of Commons Committee of Public Accounts Report, *The National Programme for IT in the NHS: An Update on the Delivery of Detailed Care Records Systems* released (July 2011- Second Report) (*'Second Report'*).

[56] UK Parliament, *Second Report,* above n55.

since 2002.[57] Other significant report outcomes included the need for the NHS Trusts to take over responsibility for care records in the UK from 2015, and the responsibility of the Department's weak project management and poor accountability style for the system failings.[58]

The present Conservative-Liberal Coalition Government in Britain introduced the Summary Care Record,[59] which store a limited range of data for all patients except those who choose not to have one. Electronic transfers are widely used for prescriptions from GP practices to pharmacies and for the storage and distribution of digital images (X-ray, scans, etc.). The 'Choose and Book' system allows patients to choose where they wish to be treated and to book an appointment online.[60] These developments had been centrally led by the Department of Health. However, since the election of the current government it appears that significant e-health progress in Britain is being stalled and that the national program is being dismantled and future developments are increasingly being left to local area authorities.[61]

---

[57] House of Commons Committee of Public Accounts, *Second Report*, above n55.

[58] Ibid.

[59] See UK Conservative Party (2015 - David Cameron Prime Minister); United Kingdom, *UK Summary Care Record* includes: current medication, adverse reactions and allergies.

[60] United Kingdom, National Health Services (NHS), *Connecting for Health 'Spine'* (2012) <http://www.connectingforhealth.nhs.uk/systemsandservices/spine> (viewed on 14/6/2012).

[61] See The Commonwealth Fund, *International Profiles of Health Care Systems Report*, above n35. For example, from 2011-2013 pay for NHS staff was frozen for all but the lowest-paid workers; initiatives have been taken to cut the costs of purchasing medical supplies, including national and regional contracts designed to achieve savings through bulk purchases; *NHS Shared Business Services*—'a joint venture between the Department of Health and a private company provides shared functions such as finance, payroll, and e-procurement for an estimated 100 NHS organisations to reduce costs of back-office services': at 37; see also J Hughes, 'Upload of NHS records suspended', *BBC News* (UK), 16 April 2010 (online) http://news.bbc.co.uk/2/hi/health/8625007.stm (viewed on 10/5/2011).

The Canadian Government has made substantial investments in the area of *EPR* and e-health since the 1997 federal budget.[62] Canada has also made the most significant progress in *EPR* and e-health system implementation through its delivery of shared diagnostic imaging between providers, a patient registry and progress in the field of provider registry, drug and laboratory capabilities and a unified push to advanced standards for computer language and messaging.[63] Canada Health *Infoway*,[64] a federally funded independent not-for-profit organisation, works with governments and health organisations to accelerate the adoption of *EPR* and other electronic health information systems (e.g. telehealth, public health surveillance).

A healthcare identifier (HI) number is used in Canada, but there exist limitations as to its use (it can only be used for health treatment), *EPR* patient enrolment is voluntary and participation in the system continues to have a 'consumer-centric' focus. Despite earlier successes and commitment by the Canadian

---

[62] Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role: Final Report on the State of the Health Care System in Canada* (2010), Volume Six, recommendations for reform in *The Federal Role in Health Infrastructure* Ottawa, (October 2002) [Chair: Michael Kirby - *The Health of Canadians – The Federal Role*, chapter 10 of the 'Kirby Report'].

[63] See Deloitte, *National E-Health Strategy*, above n5: at 21.

[64] Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role: Final Report on the State of the Health Care System in Canada* (2010) ('*Kirby Report*'), above n62; see also Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Federal Role in Health Infrastucture: Ottawa* (October 2002) ('*White Paper*'). This *White Paper* recommended and introduced strategies that would further encourage consumer and healthcare provider participation in EPR and e-health. As a consequence of these recommendations, in 2010 a public and private partnership known as the BRIDGE project was created and continues to work towards designing and standardising health technology. The *White Paper* also resulted in the establishment in 2011 by government of 'Health *Infoway*' an independent not-for-profit organisation whose main commitment includes the transformation of Canada's healthcare system through health IT. The main priorities of Canada's 'Health *Infoway*' include addressing policy issues and challenges in mainstreaming e-health services within its healthcare system and evaluating progress in the deployment and investment of these services.

Government, uptake of health information technologies has remained limited and still varies widely across Canada.[65]

The New Zealand Government began investing in *EPR* and e-health through a devolved funding model led by the 2001 'WAVE' initiative and the subsequent 2005 *Health Information Strategy* (HISNZ) group. New Zealand has one of the world's highest rates of information (IT) technology use among primary care physicians. Underpinning New Zealand's commitment to developing *EPR* systems is the recognition that various providers collect information for different purposes and as a consequence there is a recognisable need to have safe sharing and transfer of health information among users.[66] The New Zealand Government's 2011 — *National Health IT Plan* — committed to an objective that by 2014 all citizens would have electronic access to a core set of personal health information. While this plan of national IT health coverage is well advanced, it is yet to be fully realised. The National Health IT Board continues to work with a number of sector groups and receives advice from others, including consumers, clinicians and vendors. The Health Information Standards Organisation (HISO) supports and promotes the development and use of

---

[65] Department of Health, Canada, *National Physician Survey 2010* cites The Commonwealth Fund, *International Profiles of Health Care Systems 2013*, above n35: at 23-25. The *National Survey* reported in 2010 that only about one-third of Canadian physicians were using a combination of paper and electronic records, and 16 per cent were using only electronic records (there are no updated statistics on this survey): at 24.

[66] New Zealand, *Health Information Strategy New Zealand* (2009) favours a distributive approach for the safe sharing and transfer of patient electronic health information using interoperability standards set by the Health Information Standards Organisation (HISO). A distributed approach aims to enable the different systems of different providers to share information and differs from a single enterprise sector-wide approach that requires all providers use the same system, see Ministerial Review Group Report, Minister of Health (NZ) Tony Rydall, *Meeting the Challenge: Enhancing Sustainability and the Patient and Consumer Experience within the Current Legislative Framework for Health and Disability Services in New Zealand* (16 August 2009). This is a comprehensive report with 170 recommendations on how to reduce bureaucracy, improve frontline health services, and improve value in the public health and disability sector (released 16 August 2009).

health information standards to ensure interoperability between systems. Every person who uses health and disability support services in New Zealand has a national health index number as a unique identifier.

The present situation in New Zealand enables health professionals to view patient information through a single, secure, web-based system provided by District Health Boards (DHBs).[67] New Zealand is divided into four health areas and health programs primarily run through a District Health Board with a single IT Program Director for each region. Currently most health professionals use their own computers to log on to clinical workstations in order to obtain a fuller picture of a patient's information, including real-time laboratory results, radiology images and discharge information.[68] This continuing reliance on local computers (security and software programs) highlights the problem of regulating standardised *EPR* data protection and security, an issue that is further examined in later chapters of the thesis.[69]

B. *International Privacy Protection*

The dominant approach by various countries adopting e-health is to view privacy as a human right.[70] It is recognised by signatory countries in Article 12 of the *United Nations Declaration of Human Rights*, Article 17 of the *International Covenant on Civil and*

[67] New Zealand Ministerial Review Group, *Meeting the Challenge*, above n 66.

[68] New Zealand Ministerial Review Group, *Meeting the Challenge*, above n66: at 3.

[69] See chapter 3, pp70-98; chapter 4, pp99-120.

[70] See, eg, United Nations (UN), *Universal Declaration of Human Rights* (1948), GA Res 217A, 3rd sess, 183rd plen mtg, UN Doc A/810 at 71 (1948).

Political Rights (ICCPR) and Article 16 of *the United Nations Convention on the Rights of the Child* that privacy protection is a human right.[71]

The European Union's protection of privacy rights is contained in Article 8 of the *European Convention of Human Rights* and covers the right to respect for an individual's private and family life, home and correspondence —Article 12.[72] The European Court of Human Rights established a benchmark for analysis and application of Article 8 in the case *Von Hannover v Germany* in 2004.[73] In this case, the European Court set out application of Article 8 standards,[74] and recognised the 'fundamental importance of protecting private life from the point of view of the development of every human being's personality.'[75] It also noted that this right 'extends beyond the private family circle and also includes a social dimension'[76] and further that 'anyone, even if they are known to the general public, must be able to enjoy a legitimate expectation of protection of and respect for their private life'.[77]

---

[71] See *United Nations Convention on Human Rights, GA Res 217A, 3rd sess, 183rd plen mtg, UN Doc A/810 at 71* (1948); *United Nations Declaration of Human Rights*; *International Covenant on Civil and Political Rights* (1966), Art 17; *United Nations Convention on the Rights of the Child; European Convention for the Protection of Human Rights and Fundamental Freedoms* (1950), Article 17; *Universal Declaration of Bioethics and Human Rights* (October 2005) Article 1; see generally *Universal Declaration on Bioethics and Human Rights* (2005), 33rd Session of the UNESCO General Conference 19 October 2005; *Universal Declaration on the Human Genome and Human Rights* (1997), adopted by the General Conference of the United Nations Educational, Scientific and Cultural Organization on 11 November 1997; endorsed by GA Res 53/152, UN Doc A/Res/53/152 (1998); *International Declaration on Human Genetic Data* (2003); *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) reprinted in (1981) 20 *International Legal Materials* 422.

[72] United Nations (UN), *Universal Declaration of Human Rights* (1948), above n70.

[73] *Von Hannover v Germany* [2004] ECHR 294.

[74] *Von Hannover v Germany* [2004] ECHR 294.

[75] *Von Hannover v Germany* [2004] ECHR 294: at 69.

[76] *Von Hannover v Germany* [2004] ECHR 294.

[77] *Von Hannover v Germany* [2004] ECHR 294.

However despite this judgment, the extent of 'private life' still remains unclear and contested.

There is no freestanding right to privacy in the UK. The courts repeatedly rejected a common law tort of invasion of privacy.[78] This position was confirmed by the House of Lords in *Home Office v Wainwright*[79] and *Kaye v Robertson,*[80] instead of a separate tort of privacy the cause of action for breach of confidence has been extended to encompass misuse or wrongful dissemination of private information. Nevertheless UK development in the area has been influenced in recent years by the European Court of Human Rights (ECHR) and the *Human Rights Act 1998* (UK). The *Human Rights Act* incorporates the ECHR into domestic law of the UK. Another piece of legislation that impacts on UK information privacy is the *Data Protection Act 1998,*[81] enacted to ensure compliance with the 1995 European Directive[82] on the protection of individuals with regard to the processing of personal data and the free movement of such data.[83] The *Data Protection Act 1998* exemptions for small-to-medium enterprises were abolished to comply with *European Directive -95/46/EC.*[84] The *Privacy and Electronic Communications Regulations 2003,*[85] a *European Directive - 2006/24/EC* and the

---

[78] *Douglas v Hello! Ltd* [2007] 2 WLR 920: at 272.

[79] *Home Office v Wainwright* [2003] UKHL 53; [2003] 3 WLR 1137 [This case concerned the tort of privacy and battery].

[80] *Kaye v Robertson* [1991] FSR 62, Lord Justice Glidewell held that there was no common law right to privacy in England: at 6.

[81] *Data Privacy Act 1998* (UK).

[82] *Directive 2000/31/EC of the European Parliament and the Council on 2000 on the protection of individuals with regard to the processing of personal data.*

[83] *Directive-95/46/EC of the European Parliament and of the Council on 24 October 1995 on the protection of privacy* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (viewed on 23/11/2001); see also *Directive 1997/66/EC of the European Parliament and the Council on 1997 on processing of personal data and protecting personal privacy in the telecommunication sector.*

[84] *Directive-95/46/EC*, above n83

[85] *Privacy and Electronic Communications Regulations 2003* (UK).

Human Rights Act 1998,[86] were also all introduced to comply with the *European Convention on Human Rights* – Article 8.1.[87]

There is no common law tort of privacy in Canada. Consequently four Canadian provinces – British Columbia,[88] Manitoba,[89] Saskatchewan,[90] Quebec[91] and Newfoundland and Labrador[92] – have enacted statutory causes of action for invasion of privacy.[93] Basically the legislation provides that 'it is a tort, actionable without proof of damage for a person wilfully and without claim of right to violate the privacy of another person.'[94]

In Canada various instruments including the Constitution,[95] common law,[96] international obligations and legislation[97] achieve human rights and privacy protection. Although the Canadian *Charter of Rights and Freedoms 1982* does not

---

[86] European Parliament, *Directive 2006/24/EC* (15 March 2006); *Human Rights Act 1998* (UK).

[87] *European Convention on Human Rights Article* 8.1.

[88] British Columbia *Privacy Act*, RSBC 1996, c 373

[89] Manitoba *Privacy Act*, RSM 1987, c P125.

[90] Saskatchewan *Privacy Act*, RSS 1978, c P-24.

[91] Quebec *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35-37.

[92] Newfoundland and Labrador *Privacy Act*, RSNL 1990, c P-22.

[93] *Privacy Act* 1996 RSBC c 373 (British Columbia); *Privacy Act* CCSM section P125 (Manitoba); *Privacy Act* 1978 RSS c P-24 (Saskatchewan); *Privacy Act* 1990 RSNL c P-22 (Newfoundland and Labrador).

[94] See *Privacy Act* 1978 RSS c P – 24 (Saskatchewan) s2; see also *Privacy Act* 1996 RSBC c 373 (British Columbia) s1(1); *Privacy Act* CCSM section P125 (Manitoba) s2(1); *Privacy Act* 1990 RSBC c P – 22 (Newfoundland and Labrador) s3(1). The British Columbia legislation differs from the statutes in force in the other provinces in that it also protects the unauthorized use of the name or portrait of another – *Privacy Act* (British Columbia) s3. See also ALRC, Report 80, above n24.

[95] *The Constitution Act 1982* established the *Constitution* of Canada in 1982. The *Constitution* of Canada contains the Canadian Charter of Human Rights and Freedoms.

[96] *Jones v Tsige* 2012 ONCA 32 [the Ontario Court of Appeal's decision in *Jones v Tsige* recognised the tort of invasion of privacy in Canada].

[97] See, eg, *Canadian Charter of Human Rights and Freedoms* (1982) *Canada Act 1982* (UK), Schedule B: *Constitution Act 1982*, Part 1: *Canadian Charter of Rights and Freedoms* (1982); see also *Human Rights Act 1985* (Canada); *Privacy Act* 1983 (Canada); *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPEDA). PIDEDA sets out ground rules for how private sector may collect, use or disclose personal information (there is a *Memorandum of Understanding* between the Office of the Privacy Commissioner (Canadian Government) and Provincial Office of Information and Privacy Commissioner's, this *Memorandum of Understanding* is current as to 2015).

specifically guarantee a right to privacy, the Canadian Supreme Court has interpreted the right in section 8 – 'everyone has the right to be secure against unreasonable search and seizure' – to include a reasonable expectation of privacy in relation to governmental acts. Canada also has a Human Rights Commissioner who administers the *Human Rights Act 1983* as well as regulating equal opportunity under the *Employment Equity Act*.[98] Two federal laws, the *Privacy Act 1983* and the *Personal Information Protection Electronic Documents Act 2000* (PIPEDA) protect privacy.[99] The *Privacy Act 1983* imposes obligations on federal Government departments and agencies in respect to privacy rights by limiting the collection, use and disclosure of personal information. The *Privacy Act 1983* gives individuals the right to access and request correction of personal information about themselves held by these federal organisations.[100]

Individuals are also protected by the PIPEDA that sets out the rules for how private organisations may collect, use or disclose personal information in the course of commercial activities.[101] Several Canadian provinces have also separately passed

---

[98] *Employment Equity Act 1984* (Canada) [provides equal opportunities for four designated groups: women, aboriginals, disabled and other visible minority groups].

[99] Similar to Australian States and Territories legislation in Australia. Each Canadian Province has its own version of privacy and healthcare privacy protection, for example, *Personal Information Protection Act 2003* (British Columbia) [SBC 2003] Chapter 63; *Personal Information Privacy Act 2004* (Alberta); *An Act Respecting the Protection of Personal Information in the Private Sector 2015* (Quebec); *Personal Health Information Protection Act 2004* (Ontario); *Personal Health Information Privacy and Access Act 2009* (New Brunswick); *Personal Health Information Act* 2008 (Newfoundland and Labrador); see also ALRC, Report 80, above n24: at 22-25.

[100] Canadian Government, The Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada* (2012); Information & Privacy Commissioner Ontario, Canada, Ann Cavoukian and Richard Alvarez, ICD.D, President & CEO Canada Health *Infoway*, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win* (Discussion Paper, Information and Privacy Commissioner, Ontario, Canada, 2 March 2012).

[101] Ann Cavoukian, Office of the Privacy Commissioner of Canada, above n100; see also *Personal Information Protected Electronic Documents Act 2000* (Canada) (PIPEDA).

legislation to deal specifically with the collection, use and disclosure of personal information by healthcare providers and other healthcare organisations.[102]

In 2012, the Ontario Court of Appeals in a unanimous panel decision recognised the tort of invasion of privacy in *Jones v Tsige.*[103] This protection was achieved by confirming the existence of a right of action for intrusion upon seclusion. It was held in this case that such a cause of action would amount to an incremental step that is consistent with the role of the court to develop the common law in a manner consistent with the changing needs of society. These incremental processes include accelerating technological change and an individual's right to privacy. Legal scholar Peter Burns observes that there is 'a pressing need to preserve privacy, which is being threatened by science and technology to the point of surrender.'[104]

According to David Fraser, a Canadian privacy lawyer, it is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form.[105] The above observations by Peter Burns and David Fraser resonate in modern

---

[102] See above n99 for reference citation to Canadian provincial information privacy legislation.

[103] *Jones v Tsige* 2012 ONCA 32.

[104] Peter Burns "The Law and Privacy: the Canadian Experience" (2012) <http://www.privacylawyer.ca/2012/01/ontario> (viewed on 3/5/2012): at 1.

[105] David Fraser "Canadian Privacy Law: Ontario Recognizes Tort of Invasion of Privacy" (2012) (Blog) <http://blog.privacylawyer.ca/2012/01/onario-recognizes-tort-of-invasion-of.html> (viewed on 20/6/2012): at 1; see also Office of the Privacy Commissioner of Canada, *Transparency and Privacy in the Digital Age* (2014). This report argues that 'Transparency builds trust' – overshadowing other privacy issues has been the challenge in Canada and other democratic states about conserving the right of privacy of individuals in the digital era while also pursuing effective national security. Public concern has been heightened by revelations about state surveillance activities, especially among the so-called 'Five Eyes', which comprise of an intelligence alliance between Canada, Australia, New Zealand, the UK and the US: at 3. The OPC Canada noted that from June 2013 to June 2014, 'terms like 'metadata' and 'Five Eyes' previously found almost exclusively in blogs read by privacy technologists and policy experts, were vaulted into mainstream news headlines and leads': at 2.' And 'while the revelations about state surveillance provided an unprecedented view into the operations of intelligence agencies,

Australia and a thesis recommendation is that in order to ensure adequate individual privacy protection rights in Australia, there needs to be proactive and visible judicial intervention by a progressive Australian court system in order to help evolve privacy protection in light of advancing technology.[106]

Unlike Australia, which has not developed a separate tort of privacy,[107] New Zealand common law has recognised this specific action.[108] In *P v D*, the New Zealand High Court confirmed the necessary elements of a tort of privacy.[109] Later in *Hosking v Runting*, a majority of the New Zealand Court of Appeal recognised a common law tort of privacy.[110] The court found that there were two fundamental requirements for a successful claim for interference with privacy: firstly, 'the existence of facts in respect of which there is a reasonable expectation of privacy'; and secondly, the 'publicity given to those facts that would be considered highly offensive to an objective reasonable person'.[111] There have been relatively few cases in New Zealand dealing with the tort of invasion of privacy since developments in this area started in the mid-1980s.

---

they also raise important questions calling for *greater transparency'* [emphasis added]: at 9. It was also noted that 'in the end, it's not a question of "either, or" – it is possible to have both': at 9. Furthermore, 'Canadians (and the thesis argues that Australians) want greater transparency to see that these objectives are being sufficiently respected': at 9.

[106] See ALRC, Issues Paper 43, above n23; ALRC, Discussion Paper 80, above n24; ALRC, Final Report 123, above n24; see also thesis legal discussion and governance recommendations in chapter 5, pp146-163; chapter 6, pp184-234; chapter 7, pp238-260.

[107] See *Australian Broadcasting Corporation v Lenah Games Meats Pty Ltd* (2001) 208 CLR 199.

[108] *Tucker v News Media Ownership Ltd* [1986] 2 NZLR 716 [731-733]; *Bradley v Wingnut Films* [1993] 1 NZLR 415, 423; *P v D* [2000] 2 NZLR 591.

[109] *P v D* [2000] 2 NZLR 591.

[110] *Hosking v Runting* [2005] 1 NZLR 1.

[111] *Hosking v Runting* [2005] 1 NZLR 1: at 117.

The New Zealand Law Commission recommended in 2010 that development of the tort recognised in *Hosking v Runting*[112] should be left to the common law,[113] although the Commissioner did acknowledge that a statutory cause of action would make the law more certain and accessible.[114] In August 2011 the New Zealand Law Reform Commission released its fourth and final part of a detailed inquiry into the state of New Zealand privacy laws—*Review of the Law of Privacy Stage 4: Part 2*.[115] The conclusion and recommendations from this report are still under consideration by the New Zealand Government.

In New Zealand, human rights and privacy protection is located in the Constitution,[116] international conventions and treaties,[117] common law and legislation. The main Acts that apply to privacy are the *Privacy Act,*[118] *Privacy Amendment Act*[119] and later *Privacy Amendment Act.*[120] New Zealand also has a *Human Rights Act*[121] and the *New Zealand Bill of Rights Act,*[122] which also contribute to citizen rights and protection by the New Zealand Government.

---

[112] *Hosking v Runting* [2005] 1 NZLR 1.

[113] New Zealand Law Commission (NZLC), *Invasion of Privacy: Penalties and Remedies, Review of the Law of Privacy Stage 3*, Report No 113 (2010): at 91.

[114] Ibid 90.

[115] New Zealand *Bill of Rights Act 1990* (NZ); New Zealand Law Reform Commission (NZLRC), *A Conceptual Approach to Privacy* (MP 19, 2007); NZLRC, *Review of the Law of Privacy Stage 4*: *Part 2* NZLRC 123, (2011); Information & Privacy Commissioner Ontario, Canada, Cavoukian and Alvarez, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win,* above n100.

[116] *New Zealand Constitution 1986.*

[117] For example, *International Covenant on Civil and Political Rights* (ratified 1978); *Convention on the Elimination of all Forms of Racial Discrimination* (ratified 1972); *Convention on the Rights of the Child* (ratified 1993), above n76.

[118] *Privacy Act 1993* (NZ).

[119] *Privacy Amendment Act 1993* (NZ).

[120] *Privacy Amendment Act 1993* (NZ).

[121] *Human Rights Act 1993* (NZ).

[122] *New Zealand Bill of Rights Act 1990* (NZ).

Privacy and security protection has generally featured strongly in all Western countries *EPR* and e-health implementation agendas and reforms.[123] However because of the uptake of *EPR* and the obvious advantages of collecting and linking personal health records in a single, accessible database, there remain significant privacy risks. Unlike localised, paper-based patient health records, if there is a breach of security of electronic records, those records potentially become public property for millions of people. Numerous examples of this type of breach exist, including the unauthorised hacking of a confidential computer file containing the names of 4,000 HIV-positive patients in the United States (US); the deletion of ten years' worth of AIDS research in Italy by computer vandals in 1999;[124] the 2011 cyber-attack on detailed personal information records held by Sony PlayStation (even more disturbing is how long it took Sony to inform its customers that their personal information had been stolen); and the late 2012 cyber-terrorist attack on patient health records in Queensland, Australia.[125]

[123] With the exception of the U.S.

[124] See Damien McRae, "Telehealth and the Law: If Uncertainty Persists, Please Consult Your Lawyer" (1999) 6 *Journal of Medicine* 270: at 281; Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep up with Technology Changes" [2007] *University of New South Wales Review Series* 21; 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; see generally Roger Magnusson, "Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System" (2002) 24 *Sydney University Law Review* 5; Roger Magnusson, "Confidentiality and Consent in Medical Research: Some Recurrent, Unresolved Legal Issues Faced by IECs" (1995) 17 *Sydney University Law Review* 549.

[125] See Danielle Cesta, 'Hacking into Health Files' *Medical Observer* (Australia), I February 2013, 14-15; Kate Newton, 'GP Clinic Stands Firm Against Extortion Attempt from Hackers' *Australian Doctors* (Australia), 18 January 2013, 4.

Consequently the benefits of creating a national electronic health information scheme could be high but so are the risks to individual privacy if sensitive healthcare details inadvertently end up in criminal hands, the wrong hands or in the public arena.

IV. CONCLUSION

It is argued that the research undertaken in this thesis demonstrates the value of law reform to set up an *Independent Council* to support and strengthen individual healthcare privacy rights in Australia. It is argued in the thesis that implementation by the Australian Government of electronic information technology such as *EPR* and e-health represents the new dominant praxis for future provision and delivery of healthcare in Australia.[126] Significantly the government policy shift has changed the prevailing health-technology paradigm by challenging established methods of healthcare delivery systems and altering our understanding of healthcare providers. This happens because advances in new technology systems extend the responsibility and boundaries of personal healthcare information collection, usage and disclosure to include, amongst other requirements, a new class of non-health third party actors not normally privy to this information.[127]

In addition, the process of *EPR* mandates that all healthcare providers conform and 'standardise' clinical healthcare practice and 'voluntarily share' their patient notes.[128] The new requirement of 'sharing' digital patient healthcare record

---

[126] See chapter 2, pp38-67 for general discussion of evolving Government policy development of electronic records and e-health.

[127] See, for example, Roger Magnusson, "Confidentiality and Consent in Medical Research", above n124 [i.e. government, researchers, public health].

[128] See NEHTA, *Concepts of Operations,* above n1.

information means that healthcare providers now occupy a new role as information collection agents, irrespective of whether or not they choose to practice in the public or private health sector.

As a consequence of these modern day changes the proposed government electronic healthcare delivery system continues to challenge established concept of health, technology, and privacy protection — as societies morally and legally 'grapple' to understand the impact of information economy on privacy and individual privacy protection in the new global digital age. In order to fully appreciate how this shift has evolved there is a need to examine the meaning of 'symbiotic' health and acknowledge the transformational power of modern day technology, which now drives the message in healthcare privacy.

From the chapter analysis of international e-health and health privacy protection concerns there is little doubt that *EPR* and e-health system progress and implementation is an important modern day consideration given its rise in popularity in both Australia and internationally. A major concern for the public in relation to *EPR* and e-health progress is the issue of privacy and security protection.[129] New 21st century pressures found in the modern information era include: surveillance and the 'war on terror', expanding digital economy, globalisation, creation of mega data repositories, and international trade agreements,[130] which increasingly dictate the

[129] See NEHTA, *Concepts of Operations,* above n1: at 61-65; see also chapter 4, pp98-122 for discussion about the conceptual development of privacy.

[130] See Australia-US Free Trade Agreement (AUSFTA) signed in 2004; World Trade Organisation (WTO), *Dispute Settlement Understanding*, (2003), Article 8.2; Asia-Pacific Economic Cooperation (APEC); World Trade Organisation (WTO), Agreement on the Trade-Related Aspects of Intellectual Property Rights (TRIPS); see David Morris, 'Free Trade: The Great Destroyers' in Edward Goldsmith and Jerry Mander (eds) *The Case Against the Global Economy* (Earthscan Publications, 2001): at 115, TRIPS

terms of individual privacy protection in this country.[131] In order to progress the argument that individual privacy protection and ultimately democracy is threatened by expanding technologies, the thesis considers the legal and ethical impact of *EPR* and e-health on privacy and confidentiality from the Australian perspective.[132]

However, the thesis contends that how privacy is protected in a world that is moving rapidly towards 'free flow' global information, creation of unlimited individual digital profiles and surveillance mechanisms, using cyberspace communication processes remains a serious challenge, specifically in regard to individuals' right to control personal healthcare information collection, use and disclosure.

'achieving notoriety for its alleged deleterious impact on the provision and affordability of essential medicines in developing nations': at 116.

[131] See Jerry Mander, 'Technologies of Globalisation' in Goldsmith and Mander, *The Case Against the Global Economy,* above n130: at 45; see also Agnes Bertrand and Laurence Kalafatides, 'The World Trade Oganization and the Liberalization of Trade in Healthcare and Services' in Goldsmith and Mander, *The Case Against the Global Economy*, above n131: at 217; Subramanian and Katz, 'Perspectives on the Global Flow of Information' in Subramanian and Katz, *The Global Flow of Information*, above n9: at 5.

[132] See Helen Duffy, *The 'War on Terror' and the Framework of International Law,* above n21; see also Rick Sarre and Tim Prenzler, *The Law of Private Security in Australia* (Thomas Reuters, 2nd ed, 2009); Jeffery Rosen, 'The Naked Crowd: Balancing Privacy and Security in an Age of Terror' (Paper Presented at Twenty-Fourth Annual Isaac Marks Memorial Lecture, 4 March 2004).

CHAPTER 2

UNDERSTANDING THE HISTORICAL DEVELOPMENT AND CONTEXT OF HEALTH AND PRIVACY IN AUSTRALIA

This chapter provides an analysis of the health system and identifies the recent electronic health paradigm shift in Australia, extending an appreciation of electronic health information data 'collection and 'sharing' concept and its impact on individual privacy rights. It demonstrates that, despite the introduction by the previous government of privacy protection mechanisms such as legislation, technical and governance measures, privacy rights continue to be threatened in the modern

information driven technology age.[1] Alongside the expected political and legal dimension of health and privacy regulations, are evolving social and government policy considerations and the growing influence in Australia of rapidly advancing technology and globalisation.[2]

This chapter provides an incremental account of healthcare policy development including: technology, legal and governance initiatives relating to healthcare privacy, exposing the expected outcomes these changes have on privacy rights in the emerging computer information era. The contextual health and privacy *story* establishes a 'framework' in which the thesis can locate its proposition that privacy and by association democracy is under threat and further supports the recommendation that more can be done to further protect and individual advance privacy rights.

I. AUSTRALIAN HEALTH SERVICES

As a consequence of the unique historical political development of federalism, Australian health and healthcare service delivery has never been an area that promotes straightforward national policy development nor comprehensive legal

---

[1] See Australian Government, National E-Health Transition Authority (NEHTA), *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* (September 2011); see, eg, Rosemary Roberts, Kerin Robinson and Dianne Williamson, 'Health Information Policy' in Heather Gardiner and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2002): at 100; see also Evgeny Morozov, "The Real Privacy Problem" (November/December 2013) *MIT Technology Review* Vol. 116 Issue 6, 32-43; see generally Evgeny Morozov, *To Save Everything Click Here* (books.goggle.com. 2012) [Morozov challenges widespread claims that life will improve dramatically once technology makes more decisions for us].

[2] See, for example, Ramesh Subramanian and Eddan Katz (eds) *The Global Flow of Information* (New York University Press, 2011); Lawton Robert Burns (ed), *The Business of Healthcare Innovations* (Cambridge University Press, 2005); see also Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep Up With Technological Change" [2007] *University of New South Wales Law Research Series* 21; Roger Magnusson, "Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System" (2005) 24 *Sydney University Law Review* 5.

solutions. Unlike other countries not bound by the constitutional federalism,[3] Australia must always consider the numerous legal barriers and geographic state and territory limitations in relation to providing a coordinated approach to health and privacy regulation.[4] This situation often results in complicated law making and national fragmentation.[5] While it can be evidenced that some of these issues and challenges can be resolved, it is also recognised that national, state and territory political issues are dynamic, requiring sensitive and often protracted negotiation in an attempt to find agreed upon outcomes.[6] There are no simple solutions to constitutional problems of fragmented federal/state authority, and thus harmonising complex and often-conflicting health and privacy regulations across Australia in the modern era remains relevant and highly problematic.[7]

In practice healthcare delivery in Australia customarily relies on organisations including hospitals and personal professional service delivery such as medical

---

[3] See Tony Blackshield and George Williams, *Australian Constitution Law & Theory* (The Federation Press, 5th ed, 2010): at 146; see also George Williams, Sean Brennan and Andrew Lynch, *Blackshield & Williams Australian Constitutional Law & Theory* (The Federation Press, 6th ed, 2012); see Geoffrey Sawer, *Federation Under Strain* (Melbourne University Press, 1977); see *Commonwealth of Australia Constitution Act 1900*.

[4] See Linda Hancock, 'Australian Federalism, Politics, and Health' in Heather Gardiner, *Health Policy in Australia*, above n1: at 49; Carol Grbich, 'Moving Away from the Welfare State: The Privatisation of the Health System' in Gardiner and Barraclough *Health Policy in Australia*, above n1: at 79.

[5] See chapter 5 for detailed discussion on federalism and national fragmentation: at pp125-146; see Blackshield and Williams, *Australian Constitutional Law*, above n3.

[6] See Council of Australian Governments (COAG), *Joint Communique: New Council a Vital Link to Future Health Information Management Australia* (28 November 2003). The COAG *Communique,* outlined the establishment of the Australian Information Council (AHIC), its function was to provide advice on long term directions and national strategic reform issues for information management and technology in health: at 1.

[7] See Carol Grbich, 'Moving Away from the Welfare State', in Heather Gardiner, et al, *Health Policy in Australia*, above n4; George Palmer and Stephanie Short, *Health Care and Public Policy* (Palgrave Macmillan, 4th ed, 2010); see also Christopher Arup, *Innovation, Policy and Law: Australia and the International High Technology Economy* (Cambridge University Press, 1993).

practitioners and allied health professionals.[8] The hospital sector is primarily made-up of acute-care public hospitals, private hospitals, geriatric and rehabilitation hospitals and those for which the defence forces are responsible.[9] Generally health care distinguishes between primary, secondary and tertiary healthcare services and is provided outside institutions to individuals in a variety of settings by a wide range of health practitioners, including medical practitioners (doctors or physicians) who are responsible for a high proportion of primary healthcare delivery. Traditionally most doctors work in private practice on a fee-for-service basis, which means they are self-employed. However there is a growing trend towards doctors moving away from sole practice and joining larger corporate run Medical Centres as either employees or independent contractors.[10]

Beside traditional healthcare professionals such as medical practitioners and nurses there are numerous other healthcare providers, these providers predominately work in a private setting consisting of pharmacists, dentists, optometrists, physiotherapists, psychologists, chiropractors, and other healthcare workers.[11] Additionally there are other growing specialist groups outside mainstream healthcare providers influencing healthcare delivery in Australia are health economists, health analysts, public sector managers, and health epidemiologist researchers.[12] Research

---

[8] Allied healthcare professionals include – physiotherapists, nurses, social workers, psychologists, occupational therapists, etc.

[9] Palmer and Short, *Health Care and Public Policy*, above n7: at 3.

[10] Ibid 7.

[11] See, for example, Complementary Alternative Medicine (CAM) include naturopaths, acupuncture, homeopaths, etc; see Michael Weir, *Law and Ethics in Complementary Medicine* (Allen & Unwin, 4th ed, 2011); see also Julie Zetler and Rodney Bonello, *Essentials of Law, Ethics and Professional Issues for CAM* (Elsevier, 2012) 95.

[12] Jan Garrard, 'Evidence and Public Health: Data, Discourse, and Debates' in Helen Keleher and Colin MacDougall (eds), *Understanding Health* (Oxford University Press, 2nd ed, 2012): at 59; see generally

and statistical agencies provide the information needed for disease prevention, detection, diagnosis, treatment, and care associated policy.[13] These specialities are extremely influential in supporting evidence based medicine[14] research methods in health practice and contribute to government health policy planning and resource management.[15]

II. AUSTRALIAN GOVERNMENT POLICY DEVELOPMENT OF ELECTRONIC HEALTHCARE REGIMES

The necessity for the federal Government to reinvent health and healthcare delivery experience in Australia is closely linked to numerous social, political and cultural changes affecting not only Australia but also all Western liberal countries over the last few centuries.[16] As outlined in chapter 1, these events include the rise of modern neoliberal economics and globalisation involving rapid advances in computer and information technology.[17]

Roger Magnusson, "Data Linkage, Health, Research and Privacy: Regulating Data Flows in Australia's Health Information System", above n2.

[13] Australian Institute of Health and Welfare (AIHW), *Australia's Health 2010* (May 2010) 11.

[14] See Ray Pawson, *Evidence-Based Policy* (Sage Publication, 2006). ''Evidence based medicine' is founded on scientific principles and methods in contrast to information obtained from personal experience, intuition, or from anecdotal, traditional, or common sense sources': at 7.

[15] Ibid 71-72.

[16] See generally Nicholas Terry, "Electronic Health Records: International, Structural and Legal Perspectives" (2011) 12 *Journal of Law and Medicine* 26 [the article compares the progress that Europe, Australia and the United States have made in the journey towards EHR implementation].

[17] See chapter 1 for discussion of international electronic health records and e-health perspective: at pp16-36; see also Australian Government, National Health Reform Committee, *A National Health and Hospitals Network for Australia's Future Delivering the Reforms* (2010); National E-Health and Information Principal Committee, Deloitte, *National E-Health Strategy* (30 September, 2008): at 4.

Other national and local influences also challenging traditional Australian healthcare delivery modalities include: an ageing population, increasing healthcare provision costs, remote and indigenous healthcare access and equity issues, increasing migration and cultural diversity, impact of workplace gender equality, and diminishing national and local employment opportunities.[18] As a result of these challenges, over the last few decades the Australian Government has adopted a new electronic healthcare regime that clearly embraces the transformational power of computer technology and information economy technology to take Australian healthcare systems into the 21st century.

In order to capture the impact of the new electronic healthcare regime on privacy rights the chapter now turns to providing an overview of *EPR* and e-health system research, development and implementation mechanisms from 2000 to 2014. This particular period is significant because this timeline (2000-14) best exemplifies the three main stages of *EPR* and e-health conceptual progression of the system: (i) research (2000-05), (ii) development (2003-06), and (iii) implementation and uptake (2006-14). Interwoven throughout this period are architectural system design and privacy and security concerns relating to advancing health technology and general public privacy protection rights.[19]

---

[18] National Health Reform Committee, *A National Health and Hospitals Network for Australia's Future Delivering the Reforms*, above n17: at 8.

[19] See National E-Health Transition Authority (NEHTA), *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System* ('*Concepts of Operations*') (September 2011); Australian Government, *Personally Controlled Electronic Health Record System: Legislation Issues Paper* (2011); see ALRC, *Review of Australian Privacy Law:* Discussion Paper 72 (2007); ALRC, *For Your Information: Australian Privacy Laws and Practice* (August 2008); see also *Privacy Act 1988* (Cth) [which now extends privacy in areas such as public and private sector and credit reporting and healthcare information protection].

To fully appreciate the complexity of the Australian digital e-health scheme, its development and implementation needs to be recognised as an important 'revolution in healthcare'.[20] It is also necessary to understand that the e-health system consists of two complementary and equally important parallel functions.[21] Firstly it involves *EPR* and e-health architecture, which relates to system process design development and building such as interoperability, capabilities and infrastructure design (software, hardware). The second function attaches to the introduction and embedding of essential protective tools such as privacy, security and utility mechanisms needed to ensure legal protection and community confidence in the new electronic system.[22] These two functions are interdependent processes and deliver the foundational framework for the new healthcare regime.

A key element of Australia's electronic healthcare system is the ability to uniquely identify individuals, the constant collection, exchange and transmission of health information within the context of information *sharing* about a single patient being exchanged between multiple providers in a secure environment.[23] Given this focus, in the late 1990s the federal Government set out to develop and implement *EPR* and e-health systems as a national priority, gaining much needed agreement and

---

[20] See Rhonda Jolly, 'The E-Health Revolution – Easier Said Than Done' (Research Paper No 3, Parliamentary Library, Parliament of Australia, 17 November 2011) [Jolly observes that e-Health is seen by some as possibly the most important 'revolution in healthcare' since the advent of modern medicine]: at 1.

[21] See NEHTA, *Concepts of Operations*, above n19.

[22] See NEHTA, *Concepts of Operations*, above n19; see generally Australian Government, Health*Connect*, Health*Connect Interim Report: Overview and Finding* (2003); Australian Government, Health*Connect*, Medi*Connect*, *Lessons Learned from the MediConnect Field Test and HealthConnect Trials* (April 2005); NEHTA, *Healthcare Identifiers Service Implementation Approach* (2010); NEHTA, *Frontiers in Healthcare Delivery* (2007); Australian Government, *National Health Reform: Progress and Delivery* (September 2011).

[23] See NEHTA, *Concepts of Operations,* above n19.

cooperation from the State and Territory Governments.[24] As part of the process of introducing *EPR* and e-health systems, federal Governments[25] have commissioned reports and research, established advisory councils and statutory authorities, and invited public and stakeholder submissions on the viability and impact of e-health projects.[26] As a consequence the policy of e-health implementation and its many benefits has been generally endorsed by governments of all political persuasions and at all levels.

III. 'GRAND PLAN' FOR AUSTRALIA – TOWARDS NATIONAL COORDINATION OF E-HEALTH

---

[24] See Commonwealth Government, Department of Communication, Information, Technology and the Arts, *Information Economy: Identifying Priorities of Action* (December 1998). This report identified key issues and priorities of action for a national direction of 'harmonisation' needed for the modern information economy; Commonwealth Government, *Health Online: A Health Information Action Plan for Australia* (November 1999); Commonwealth Government, *Health Online* (September, 2nd ed, 2001). Health online promotes new ways of delivering health services by harnessing the enormous potential of new and emerging online technologies, including internet-based communication. It also commits government to the development of an environment in which privacy and dignity of individual health consumers is paramount: at 2. Commonwealth Government, National Electronic Health Records Taskforce, *A Health Information Network for Australia* (July 2000). In June 2000 the National Health Information Standards Advisory Committee (NHISAC) was formed. The NHISAC had a policy role that straddled both public and private sectors and gave advice to Health Ministers on health information standards; see NHISAC, *Setting the Standards: A National Health Information Standards Plan for Australia* (February 2001). [Please note that elected Government refers to both the Australian federal Labor Party and the federal Coalition Liberal Party when they held power]; see Council of Australian Government (COAG), *National Health Agreement 2011* (2011); COAG, *National Agreement 2012-2013* (2012); see also COAG, *Joint Communique*, above n6 [This is an agreement between governments to work together in the provision of healthcare delivery between the Commonwealth of Australia and the States and Territories, being: NSW, Victoria, Queensland, Western Australia, South Australia, Tasmania, ACT and the Northern Territory of Australia].

[25] See timeline of Australia's Prime Ministers: 1972-75, Gough Whitlam (Australian Labor Party); 1975-83, Malcolm Fraser (Coalition Liberal Party); 1983-91, Robert Hawke (Labor Party); 1991-96 Paul Keating (Labor Party); 1996-2007, John Howard (Coalition Liberal Party); 2007-2010, Kevin Rudd (Labor Party); 2010-2011, Julia Gillard (Labor Party); 2011-2013, Kevin Rudd (Labor Party); 2013 – Tony Abbott (Coalition Liberal Party).

[26] See, for example, NEHTA, Health*Connect*, Australian Law Reform Commissioner (ALRC), Office of the Australian Privacy Commissioner (OAPC), Australian Privacy Foundation and other stakeholders.

Governmental collaboration commenced in December 1998 when the federal Department of Communications, Information and the Arts released — *Information Economy: Identifying Priorities of Actions* on e-health.[27] This action plan was later endorsed by the National Health Information Management Advisory Council (NHIMAC), which was given a number of tasks intended to address the barriers to e-health. In response to this challenge NHIMAC conceived a 'grand plan' for e-health and released a strategy document in 1999, *Health Online.*[28] This document outlined a framework for the new information economy, which included a plan for a series of wide-ranging *National Action Strategies.* These documents were endorsed by the Commonwealth and State/Territory Governments through the *Online Council* (health being one area of interest).[29]

In 2000 the National Electronic Health Records Taskforce (NEHRT), a sub-committee of NHIMAC was established. In July 2000, the NEHR Taskforce[30] proposed the setting-up of a national health information network – Health*Connect*. In 2001 the project received federal funding of AUD $128.3 million over four years to 'develop a secure national health information network.'[31]

---

[27] Department of Communication, Information, Technology and the Arts, *Information Economy*, above n24; Commonwealth Government, *Health Online: A Health Information Action Plan for Australia*, above n24.

[28] Australian Government, National Health Information Management Advisory Council, *Health Online: A Health Information Action Plan for Australia,* above n24.

[29] Department of Communication, Information, Technology and the Arts, *A Strategic Framework for the Information Economy: Identifying Priorities for Action,* above n24.

[30] National Electronic Health Records Taskforce (NEHR), *A Health Information Network for Australia: Report to Health Minister by the National Electronic Health Records Taskforce* (July 2001); see also National Health Information Standards Committee (NHISAC) [established at the same time as the NEHR Taskforce, the NHIMAC's function included policy advice to COAG Health Ministers that straddled both public and private sectors].

[31] See National Health Information Management Advisory Council Review Steering Group, *Review of the National Health Information Management Advisory Council: Issues Paper* (2002).

A. *Putting the 'grand plan' into action*

Health*Connect* represented a joint government initiative in partnership with the federal, states and territories funded for two years in order to investigate, trial, evaluate and recommend a national health information network, drawing on the potential of electronic health records as a way of improving the flow of information at the point of care. Health*Connect* was conceived as an overarching 'national change management strategy working towards interoperability of electronic health information products and services for health care and consumers.'[32]

Initially it was intended that the first stage of Health*Connect*, the Better Medication Management System (BMMS), would commence in July 2001. It was envisaged that under the BMMS, Medicare numbers[33] would be used to create a personal electronic medical record, which linked prescriptions with medications written by different doctors and dispensed by different pharmacies. The scheme's advantages included the minimisation of medication misadventure and prevention of doctor-shopping.[34] However there were widespread concerns within the medical

---

[32] See Australian Government, Health*Connect*, Health*Connect and the Information Management and Information Communications Technology Industry* (2003).

[33] Medicare (Australia) is a system of fee-for-service payments provided for by the Commonwealth Government for the provision of specified health services by doctors, dentists, optometrists, chiropractors, physiotherapists, osteopaths and podiatrists, including diagnostic services such as laboratory tests and scans. Generally only Australian residents are entitled to a Medicare number (card) for the provision of these health services. The Pharmaceutical Benefits Scheme (PBS) medications include prescription drugs subsidised by the Australian Government. However, not all prescription drugs (and over-the-counter drugs) are available under the PB Scheme.

[34] See Australian Medical Association (AMA), to the Senate Standing Committee on Constitutional and Legal Affairs on *Submission to the Commonwealth Department of Health and Aged Care: The Better Medication Management System: Draft Exposure Legislation* (July 2001). Medical misadventure can be described as a situation where a patient has been prescribed at different time's drugs, which in combination may have an adverse side effect. Doctor-shopping is when a patient visits a number of doctors generally over a short period of time to obtain multiple prescriptions from the different doctors in order to procure certain restricted drugs such as sedatives and opiates: at 5.

community about the BMMS, especially relating to the inclusion of necessary privacy protection.[35] As a result, a limited number of field tests to encourage provider and consumer participation in Medi*Connect* (BMMS) were conducted at sites in Tasmania and Victoria.[36]

Further to the BMMS Medi*Connect* field tests, Health*Connect* would also be involved in a series of live trials to determine how a future health information network would function. The Health*Connect* goals were shaped by a set of seven high level research questions aimed at 'testing the value, technical feasibility, preferred implementation model, sustainability of Health*Connect* as a national approach to electronic health records'.[37] These questions were:

1. Can Health*Connect* prove its value?
2. Is Health*Connect* technically feasible?
3. Is there a preferred implementation model?
4. What role should the private sector play?
5. What will be necessary to manage privacy?
6. How should Health*Connect* be governed?
7. What will Health*Connect* cost and is it sustainable? [38]

In order to test the effectiveness of these questions, Health*Connect* conducted several trials in selected areas around Australia. The trials were run in Queensland, NSW, Tasmania and the Katherine region of the Northern Territory. The Tasmanian trial

---

[35] See Department of Health and Ageing, Medi*Connect: Linking Medicines Information: Report* (January 2005).

[36] AMA, *Submission to the Commonwealth Department of Health and Aged Care, The Better Medication Management System*, above n34.

[37] See Australian Government, Health*Connect* Program Office, *Consent and Electronic Health Records: A Discussion Paper* (July 2002); See also Australian Government, Health*Connect*, *Interim Research Report: Overview and Findings* (August 2003); Australian Government, Health*Connect*, *What is* Health*Connect?* (November 2003).

[38] Health*Connect* Program Office, *Consent and Electronic Health Records: A Discussion Paper*, above n37.

focused on adults with diabetes and involved a wide range of services.[39] The Queensland and Katherine region trials focused on Indigenous health issues associated with mobile population in a remote region.[40]

Both Health*Connect* research trials and Medi*Connect* field test represented a major priority for progressing *EPR* – and was instrumental in developing key 'building blocks' needed for the broader e-health agenda such as consent, privacy and technical and information standards.[41] In July 2002 the Health*Connect* Program Office released a discussion paper, which set out a number of key concepts and issues in relation to the proposal for the Health*Connect* project.[42] This document highlighted the importance of privacy, access, security, and secondary information usage and consent requirements. Strategic recommendations included: building on the consent and access control policy by further developing the broader privacy framework, including enacting specific legislation for Health*Connect*.[43] The Health*Connect* recommendation that there should be specific legislation in the health privacy area is further discussed in chapter 5, where it is argued that such legislation would help strengthen individual privacy protection in Australia.

In November 2002 Council of Australian Governments (COAG) agreed to fund a further 2 year phase of research and development. The purpose of this extended

---

[39] Health*Connect*, *Consent and Electronic Records*, above n38.

[40] Health*Connect* Program Office, *Consent and Electronic Health Records: A Discussion Paper*, above n37; see also Health*Connect*, *Interim Research Report: Overview and Findings*, above n37; Health*Connect*, *What is HealthConnect?* above n37.

[41] Health*Connect* Program Office, *What is HealthConnect?* above n37: at 1.

[42] See Health*Connect*, *Consent and Electronic Records: A Discussion Paper,* above n37: at 42-43.

[43] Ibid 43.

phase was to finalise the Health*Connect* research and architecture, continue on-going trials and begin further testing and evaluation of trials.[44] It also agreed to further develop the Health*Connect* building blocks to provide safe and secure exchange of health information for the new proposed *EPR* regime.[45] Notably during this research and evaluation period patient informed consent and privacy and its management assumed central importance in the overall design of the new system. This concern is reflected in the design of the research questions and features prominently in the results and evaluation process.

B. *Lessons learnt — HealthConnect trials and MediConnect field test*

Findings from the trials were used to inform the Health*Connect* Implementation Strategy document released in July 2005.[46] The resulting feedback from the Trials and Field Test provided essential evaluation material for Health*Connect* to consider. Common features of all the trials and field test included opt-in participation, informed consent, privacy and consent withdrawal option. Privacy and consent issues emerged as a major concern for all trials and test stakeholders.[47] The project endorsed a strong

---

[44] Australian Government, Health*Connect*, *New South Wales (NSW) and Queensland HealthConnect and MediConnect Trials 2004-2005* (2005). It was noted by researchers that consent represents an important aspect of the management of consumer privacy, and that 'the interrelationship between privacy and consent often makes separating out these issues in terms of evaluations very difficult for the Field Test and Trials': at 41; see, eg, Medi*Connect* Field Test Evaluation — Launceston Phase 1 (October 2003) (M2); Medi*Connect* and Health*Connect*, Evaluation of the Field Test of Medi*Connect*: Fourth Evaluation Field Visits to Launceston and Ballarat (November 2004) (M7); Health*Connect* North Queensland Trial Qualitative Feedback (November 2004) (Q2); Health*Connect* Northern Territory Interim Report (February 2003) (NT2); Tasmanian Health*Connect* Trial Phase 1: Final Report (August 2003 (T4); Tasmanian Health*Connect* Trial Phase 2: Final Report (November 2004) (T8).

[45] Health*Connect*, *Consent and Electronic Health Records: A Discussion Paper*, above n37.

[46] Health*Connect*, *Consent and Electronic Health Records*, above n37.

[47] Ibid.

'consumer centric' consent model.[48] Emphasis was placed on both health consumer and healthcare providers to deliver informed consent obligations. Further, to ensure that these obligations were met the trials and field test participants were provided with extra practical resources such as access to ongoing education/training, resources and time needed to educate healthcare providers and recruit participants.[49]

Feedback from health providers to trial organisers reported that the process for informed consent was labour intensive and had the potential to confuse rather than enlighten participants.[50] Obligations in time and cost attached to obtaining informed consent from consumers by health providers represented a significant practical and economic commitment. It was noted that some health providers (particularly doctors and pharmacists) viewed the requirement for obtaining informed consent prior to inclusion of data in e-health as a 'burden'.[51] It was strongly indicated by some health providers that at this level of involvement including the responsibility for obtaining consent for Health*Connect* and Medi*Connect* inclusion should not rest with them.[52]

---

[48] See Health*Connect*, Dr Brian Richards, National Director E-Health Implementation Australia, *E-Health Implementation Stakeholders Perspective* (25 November 2005).

[49] See Australian Government, Health*Connect*, *New South Wales and Queensland HealthConnect and MediConnect Trials 2004-2005*, above n44. A feature of the Health*Connect* trial and field test was that research assistants were able to meet and spend quality time with individuals in their homes (or surgery, pharmacy) in order to fully explain the consent process and requirements of the study to research participants; see Health*Connect*, *Consent and Electronic Health Records: A Discussion Paper*, above n37; see generally Australian Health Information Council (AIHIC), *E-Health Future Directions Briefing Paper* (4 October 2007).

[50] Australian Government, Health*Connect*, *New South Wales and Queensland HealthConnect and MediConnect Trials 2004-2005,* above n 44: at 39; see also Health*Connect*, *Consent and Electronic Health Records*, above n37.

[51] Health*Connect*, *Evaluation of the Field Test of MediConnect* (January 2005) [It was reported by healthcare providers (doctors and pharmacists) in the 'Lessons Learnt' report that gaining informed consent added up to 'at least another ten minutes to the standard consultation time']: at 100.

[52] Health*Connect*, *New South Wales and Queensland HealthConnect and MediConnect Trials*, above n44.

What emerged from the trials reinforced the notion that consent and privacy concerns in *EPR* remained an ongoing issue for the community.[53] It is important to note that secondary use of the Health*Connect* repository information (such as research, secondary use, health service planning and consumer selection for clinical trials) where not explored in these initial trials and field tests. The adoption of Health*Connect* represents phases 1 and 2 – research and development of the continuing national e-health system project.

C. *Moving one step closer – e-health design and implementation plans*

In 2004 the Boston Consulting Group (BCG), which had been commissioned to report/provide advice, advised the federal Government that a further problem in implementing a comprehensive e-health program was that there were too many small, loosely coordinated e-health initiatives underway across the different state and territories in Australia and what was needed was a central collaborative body.[54] It was partly in response to the BCG report that in July 2005 the National E-Health Transition Authority (NEHTA) was formed.[55]

During 2003-2005 the federal Government recognised that *EPR* implementation was not progressing quickly enough. NEHTA was created to help expedite the process. NEHTA is a not-for-profit company with 3 year tenure jointly funded by

---

[53] See Medical Observer Editorial, 'Your Obligations, for the Records' *Medical Observer* (Australia), 28 September 2007, 43.

[54] See Boston Consulting Group (BCG), *National Health Information Management and Information and Communications Technology Strategy* (August 2004) [The National Health Report prepared for the Australian Health Information Council by the Boston Consulting Group (BCG)].

[55] Boston Consulting Group (BCG), *National Health Information Management and Information*, above n54; see also David Moore, 'Health*Connect* is Dead. So Now What?' *New Matilda* (*Magazine)* (Australia), 1 February 2006, 1.

Australian State, Territorial and federal Governments.[56] It has responsibility for developing national health Information Management (IM) and Information and Communication Technology (ICT) standards and specifications.[57] The Board of NEHTA is comprised of chief executives from federal, state and territory health departments. Since its inception NEHTA has attracted COAG funding for three key building blocks initiatives:

1. The HealthCare Provider Identifier;
2. The Individual Healthcare Identifier;
3. Shared Electronic Health Records.[58]

It was agreed upon by federal, State and Territory Government in 2005 that as part of the national coordination plans, NEHTA would focus on accelerating healthcare reform and develop national standards, specifications, terminologies and format to enable interoperability, identify and fund the 'missing pieces' of infra-structure in healthcare Identifiers and clinical terminology, develop the national policies required

---

[56] See Review Panel, Richard Royle, Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013) recommended (Rec. 1) that NEHTA be abandoned and a new structure be created. At time of writing the *Royle Review* recommendations had not yet been implemented by the current federal Coalition Government (April 2015). See chapter 6, pp184-234 for further discussion of the *Royle Review - PCEHR* and e-health governance recommendations and future plans; see chapter 7, pp250-260.

[57] Information Management (IM) and Information & Communication Technology (ICT) standards refer to the standard based-approach existing in Australia and internationally accepted relating to technical specifications of standards adopted for computer communication conformity; BCG, *Report on the NEHTA Review* (October 2007). The standards adopted were SNOMED CT for clinical terminologies and HL7 V2x for messaging.

[58] See Australian Health Minister's Conference, Council of Australian Governments (COAG), $18.2 million (over three years) (28 January 2005); Council of Australian Governments (COAG), $130.2 million (over four years) (10 February 2006); Council of Australian Governments (COAG), $218 million (over three years) (29 November 2008); Commonwealth Budget Review 2010-11 *Budget* the Government committed funding of $466.7 million (over two years) to establish key components of a *PCEHR* system; Budget for health record initiatives $233.7 million (over three years); see also NEHTA, *Privacy Blueprint for Individual Electronic Health Record* (3 July 2008); NEHTA, *Privacy Blueprint for the Individual Electronic Record* (February 2006); NEHTA, *NEHTA's Approach to Privacy* Version 1.0 (4 July 2006); NEHTA, *E-Health Record: Shaping the Future of Healthcare* (September 2008).

to protect privacy and patient consent; as well as establish a basis for modelling benefits from e-health to assist in assigning investment priorities.[59]

NEHTA in 2006 outlined its broad overview of its position on privacy in its *Approach to Privacy* and *Privacy Blueprint – Unique Healthcare Identifiers* and in its 2008 *Privacy Blueprint for the Individual Electronic Health Record*, which set out a systematic framework to consider privacy issues raised by the collection and use of information involved with the Unique Healthcare Identifiers (UHI) service. NEHTA committed to developing an effective privacy framework for *EPR* and e-health, acknowledging that these must comply with both privacy legislation and community expectations.[60] It also considered that Australian privacy legislation could be navigated but recognised that this was both high-risk and highly complex due to the 'patchwork' of legislative coverage in Australia and the requirement to apply privacy principles to specific situations, rather than read them as statutes.[61]

---

[59] See NEHTA, *Latest News-Software Developers to Engage with National E-Health Records System Ahead of July 2012 Launch* (July 2012) ; see also BCG, *National Health Information and Management*, above n54: at 4.

[60] NEHTA, *E-Health Healthcare Today* (July 2010): at 5, 8; Australian Health Information Council (AHIC), *E-Health Future Directions Briefing Paper for AHMAC Meeting* (4 October 2007): at 9; see also *Privacy Act 1988* (Cth).

[61] NEHTA, *E-Health Healthcare Today*, above n60; see generally Australian Government (COAG), *A National Health and Hospitals Network for Australia's Future: Delivering the Reform* (June 2010). Under the National Health and Hospitals Network, the Commonwealth will become the majority funder of the Australian public hospital system. Implementation will be built around close cooperation between the Australian Government and State and Territory Government: at 6. See also COAG, *Australian Health Ministers Cooperation towards National Health Care* (April 2010). The *National Healthcare Agreement 2011* establishes principles for the operation of health systems such as: 'provide timely access to quality health services based on need, not ability to pay, regardless of geographic location; adopt an integrated approach to health; focus on prevention not just treatment and address the needs of patients, families and communities': at 1.

D. *Deloitte Report*

In 2006 the Australian Government commissioned an e-health strategy report from Deloitte.[62] The Deloitte National E-Health and Information Principal Committee[63] delivered its completed report, *National E-Health Strategy* (*'Deloitte Report'*) in late 2008. In 2009 the federal Government wholeheartedly adopted the *Deloitte Report* recommendations, including the creation of a legislative framework to govern the roll out of electronic health identifiers.[64] However, in response to the *Deloitte Report* legal academic, Danuta Mendelson, observed that the report and the Government's new strategy 'painted a picture of electronic health care utopia, in contrast to the miserable present state of not-sufficiently IT driven medical practice.'[65] Mendelson was not convinced that Deloitte made a sufficiently compelling case to the Government to prompt spending billions of dollars to implement the e-health recommendations and strategy outlined in the report.[66]

E. *Australian Law Reform Commission*

In 2008, during the *EPR* research and development period, the Australian Law Reform Commission (ALRC) completed a 28 month inquiry into the effectiveness of Australian privacy law.[67] The report provided an overview of privacy law and

---

[62] Deloitte, *National E-Health Strategy,* above n17. Deloitte is a professional service firm, providing audit, tax, consulting, and financial advisory services: at 3.

[63] The committee is not listed by name.

[64] See Danuta Mendelson, "Healthcare Identifiers Legislation: A Whiff of Fourberie" [2010] 17 *Journal of Law and Medicine* 664.

[65] Deloitte, *National E-Health Strategy*, above n17.

[66] See Rhonda Jolly, 'The E-Health Revolution – Easier Said than Done', above n20 cites Danuta Mendelson, "Healthcare Identifiers Legislation", above n64: at 29.

[67] ALRC, *For Your Information: Australian Privacy Laws and Practice* (August 2008); ALRC, Executive Summary, *Extensive Public Engagement:* Report 108 (11 August 2008); see generally ALRC, *Serious*

regulations in Australia and made 295 recommendations for improving general privacy protection in public and private sectors, noting 'Australians do care about privacy, and they want a simple, workable system to provide effective solutions and protections.'[68] A later ALRC report published in 2009 — *For Your Information: Australian Privacy Law and Practice* and 2014 — *Serious Invasions of Privacy in the Digital Era* — also highlights the importance of privacy protection for Australian.[69]

Of these 297 ALRC general recommendations, 197 elicited a response by the Australian Government.[70] The main healthcare privacy recommendations included: enhancing the *Privacy Act 1988* (Cth), name, structure, objects, definition and scope;[71] developing unified national privacy principles; and reviewing the powers of the Office of the Australian Privacy Commissioner.[72] In 2009 the Australian Government released its first stage response report to the ALRC– *Enhancing National Privacy Protection: Australian Government First Stage Response to the ALRC Report 108*[73] – in

Invasions of Privacy in the Digital Era: Discussion Paper 80 (31 March 2014); ALRC, *Serious Invasions of Privacy in the Digital Era:* Final Report (September 2014) [this Report set out Terms of Reference for an inquiry into the protection of privacy]; ALRC, *Privacy Law and Practice* (25 June 2006) [this 28-months inquiry looked at the extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for Australian privacy]; ALRC, Review of Australian privacy Law: Discussion Paper 72 (September 2007) [this Discussion Paper 72 provides a comprehensive background to the rights of privacy in Australia]; see also New South Wales Law Reform Commission (NSWLRC), Consultation Paper 1: *Invasion of Privacy* (May 2007).

[68] ALRC, *Review of Australian Privacy Law:* Discussion Paper 72, above n67: at 97.

[69] ALRC, *For Your Information: Australian Privacy Laws and Practice:* Report No 32, above n67.

[70] Australian Government, *Enhancing National Privacy Protection: Australian Government's First Stage Response to the ALRC: Report 108* (October 2009). The ALRC made 295 recommendations, the Australian Governments first stage response addressed 197: the Government accepted 141 of the ALRC recommendations, either fully or in principle, 34 recommendations are accepted without qualification, 20 recommendations were not accepted and a further 2 recommendations are noted for further consideration.

[71] ALRC, Discussion Paper 72, above n67: Rec. 3-1, 8-3.

[72] ALRC, Discussion Paper 72, above n67: Rec. 15-1 – 16-1, Rec. 18-1 -44-1, Rec. 46-1 – 50-4.

[73] Australian Government, *Enhancing National Privacy Protection,* above n70.

which it committed to establishing 'a clear and simple framework for privacy rights and obligations and build on its commitment to trust and integrity in Government.'[74]

The outcome of the federal Governments' first stage response to the ALRC recommendations resulted in legislation such as the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) and the *Personally Controlled Electronic Health Record Act 2012* (Cth) (*PCEHR Act*); as well as its subsequent 12 March 2014 introduction of a single set of National Privacy Principles (13 Australian Privacy Principles (APPs)).[75]

F. *Office of Australian Information Commissioner*

On 1 November 2011 the Office of the Australian Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC). A function of the OAIC is to protect information rights and advance information policy. This function is further clarified and strengthened with new *Privacy Act* amendment laws.[76] The OAIC regulates the handling of personal information under the e-health record system by individuals, Commonwealth Government agencies, private sector organisations and some State and Territory agencies.[77] The OAIC's role also includes investigating complaints about mishandling of health information in an individual's e-health record. The OAIC is able to conduct its 'own motion investigations' and the functions and enforceable powers available to the OAIC include the right to seek a civil penalty from the Courts, seek an injunction to prohibit or require particular

[74] Australian Government, *Enhancing National Privacy Protection*, above n70: at 6.

[75] See chapter 5, pp174-182 for discussion of e-health and privacy legislation.

[76] See, for example, *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)

[77] Office of Australian Information Commissioner (OAIC), *The E-Health Record System* (2011): at 1.

behaviour. It is also able to accept enforceable undertakings and use existing *Privacy Act* investigative and enforcement mechanisms including conciliation of complaints and formal determinations and accepting data breach notifications from the System Operator, Repository Operators and Portal Operators.[78]

However recent policy strategies by the current Coalition Liberal Government contained in the 2014 federal *Budget* has resulted in rationalisation of services for the Office of the Australian Information Commission (OAIC) and the partial disbandment of COAG functions. This 'rationalisation' objective has the potential to severely affect the funding and governance resources of the Information Commissioner, particularly in its extended role under the current legislation in maintaining electronic health records privacy compliance, complaints handling and guidance.[79]

G. *National Health and Hospitals Reform Commission Report*

---

[78] OAIC, *The E-Health Record System*, above n77: at 1-2; see, for example, OAIC, *Privacy Impact Assessment Guide* (2006). The OAIC released a document outlining *Privacy Impact Assessment Guide* (PIA). The OAIC claims that a PIA is important because it 'tells the story' from the privacy perspective and helps manage privacy impacts. It is recognised that if privacy issues are not handled properly that this can have detrimental consequences on the community trust and undermine the project's success. The PIA Report is designed to help identify what needs to be done to ensure that a project such as PCEHR and e-health complies with privacy laws and other legislative requirements. The main healthcare legislation PIA Reports over a three year period (2006-2009) include: Galexia, *Preliminary PIA Healthcare Identifiers and Individual Healthcare Provider Final Report v19* (7 May 2006) Clayton Utz, *National E-Health Transition Authority Unique Healthcare Identifier Program Privacy Impact Statement* (3 March 2008) and Mallesons, Stephens, Jacques, *Privacy Impact Assessment Individual Healthcare Identifiers* (July 2009) - PIA Government Commissioned Reports.

[79] See *Healthcare Identifiers Act 2010* (Cth) and *Personally Controlled Electronic Health Record Act 2012* (Cth) (*PCEHR Act*). Both the *Healthcare Identifiers Act* and *PCEHR Act* extend the privacy protection role and function of the Australian Privacy Commissioner. In 2000 the then federal Coalition Government engaged in rationalising resources to the Australian Privacy Commissioner, which impacted negatively on its ability to effectively implement privacy law changes brought about under the *Privacy Amendment (Private Sector) Act 2000* (Cth). Under the private sector amendment changes the Privacy Commissioner was now required to overview and provide guidelines for not just the public sector but also for the private sector.

The ongoing task of developing a long-term health plan and reform platform for Australia was entrusted by Government to the National Health and Hospitals Reform Commission (NHHRC) – *A Healthier Future for all Australians*.[80] Despite ongoing concerns about the *Deloitte Report* expressed by Mendelson,[81] the Government endorsed the NHHRC's proposed directions for *PCEHR* and e-health, which were in line with the *National Health Strategy* report. The Commission also set a July 2012 deadline for NEHTA in relation to the introduction of a consumer *PCEHR* system and implementation of e-health in Australia by 2015.[82]

Included in the 2010-11 federal *Budget* the Commonwealth Government announced it would spend AUD $466.7 million over two years to create a *PCEHR* for every Australian. The funding was intended to establish a secure system of *PCEHR* that would provide: summaries of patient's health information; secure access for patients and healthcare providers to their e-health records; and rigorous governance and oversight to maintain privacy. It would also establish Lead implementation sites comprised of health sector organisations. These health and community partnerships would focus on implementing *PCEHR* components that support sharing or aggregation of electronic health information at a geographic or sector functional level, such as health record repositories, discharge summary capabilities or medications management capabilities.[83]

---

[80] See NHHRC, *A Healthier Future for all Australians: Final Report* (June 2009).

[81] See Danuta Mendelson, "Healthcare Identifiers Legislation", above n64.

[82] NHHRC, *A Healthier Future for all Australians*, above n80; Australian Government, *A Health Information Network for Australia*, above n24.

[83] NEHTA, *PCEHR Lead Sites* (2012). The nine organisations selected to develop a Project Implementation Plan were: Accoras, NSW Department of Health, Cradle Coast Electronic Health Information Exchange (Tasmania), Calvary Health Care ACT Limited, A consortium of Government,

In August 2010 NEHTA selected three organisations as lead sites to deploy and test national e-health infrastructure and standards, demonstrate tangible outcomes and benefits from funded e-health projects, and build stakeholder support and momentum behind the *PCEHR* program.[84] These three sites were part of the first wave lead sites and the second lead sites were selected later in March 2011.[85]

H. *McKinsey and Company – adoption partner*

As part of the *PCEHR* system implementation process the then federal Health Minister, Nicola Roxon, announced the Government would invest part[86] of its $466.7 million in *PCEHR* project money in contracting a change and adoption partner. This it rationalised would help take *EPR* and e-health to the next level of functionality, interoperability, implementation and uptake. The appointment of McKinsey and Company to lead a consortium to input into the proposed *PCEHR* legislation and help support, educate and change manage health workers using the system at 12 lead implementation sites was contracted.[87]

GP Networks and Aboriginal run health services from the NT, SA and far north WA, St Vincent and Mater Health Sydney Limited, Fred IT Group Pty Limited, Medibank Private Limited, and Mater Shared Electronic Health Record.

[84] Ibid [these Lead Sites are: Hunter Urban Division of General Practice, GP Partners Limited, and Melbourne East General Partners Network Limited to work with NEHTA to prepare implementation plan proposals for lead implementation project. Wave 1-Commonwealth has provided funding to Hunter Urban Division of General Practitioners, GP Partners Limited, and Melbourne East GP Network Limited to prepare implementation plan proposals for lead implementation project. Wave 2- the key objectives of these e-health sites are to achieve national demographic coverage, widespread coverage across healthcare sectors, deliver early benefits and demonstrate new and innovative concepts].

[85] Ibid.

[86] See Australian Government, *Healthbase Australia*, *Personally Controlled Electronic Health Records*, *Change and Adoption Partner -$29.9 Million* (2012). The adoption partner contract is worth $29.9 million.

[87] Fran Foo, 'Team McKinsey Bags Major E-Health Deal' *The Australian* (Australia), 7 July 2011, 10.

NEHTA considered that the change and adoption partner, McKinsey and Company would leverage health sector and ICT industry knowledge and capability to inform the roll out of the *PCEHR* Program, develop a national change and adoption strategy for the rollout of the *PCEHR* Program encouraging adoption and uptake by healthcare providers and citizens of the System. It would also help utilise and leverage existing stakeholder engagement forums and networks, and lead the delivery of the *PCEHR* program marketing and communications campaign in line with the marketing and communication strategy provided by the Department of Health and Ageing (DoHA) and NEHTA.[88]

Further in March 2011 NEHTA selected nine organisations as part of the second wave of lead sites.[89] A key objective of the second wave was to achieve national demographic coverage. Consequently in April 2011 NEHTA released the *Draft Concept of Operations for the PCEHR System* for public comment and later in September 2011 the *Concept of Operations PCEHR* was published. The system architecture, legislative proposals and governance-operating model to support the *PCEHR* System were laid out in these documents.[90]

IV. MARCHING FORWARD - NEHTA's 'CONCEPT OF OPERATIONS'

[88] Australian Government, *Healthbase Australia*, *Personally Controlled Electronic Health Records,* above n86: at 1.

[89] See NEHTA, *PCEHR Lead Sites*, above n83.

[90] NEHTA, *Concepts of Operations,* above n19 [the *Concepts of Operations* document sets out the legislation reform discussion]: at 63-65; and the governance operating model discussion: at 102-103.

The *PCEHR* system enables the collection of information from participating organisations, individuals and the Department of Human Services Medicare program within a series of conformant repositories.[91] NEHTA's response regarding privacy and security issues was set out in the draft and final 2011 *Concept of Operations: PCEHR System* relating to the introduction of a *PCEHR* system and its addendum.[92] The report was designed to provide an overview of the *PCEHR* system and how it would look and work. It envisaged that the document would be periodically updated as the development of the *PCEHR* system progressed.[93] The scope of the concept report covers aspects of requirements and design, legislation and governance, change and adoption, and benefits and evaluation.[94]

A foundational component of *PCEHR* implementation is the allocation of healthcare identifiers. In 2009 COAG agreed to establish and fund the *PCEHR* Service Operator responsible for the set-up and maintenance of the Identifier Health System, a position that was awarded to Medicare Australia. This role forms part of the infrastructure for the introduction of patient-controlled individual healthcare records. Under Part 2, s9 of the *Healthcare Identifiers Act 2010* the 'Service Operator' is authorised to assign a number (HI) to uniquely identify healthcare providers and healthcare recipients.[95]

---

[91] NEHTA, *Concepts of Operations*, above n19: at 43.

[92] Ibid 43-44.

[93] Ibid 9.

[94] Ibid.

[95] See chapter 5, pp174-182; pp175-178 for discussion of the *Healthcare Identifiers Act 2010* (Cth); pp174-178 *Personally Controlled Electronic Health Records Act 2012* (Cth) (*PCEHR Act*); and pp174-180 the role of PCEHR Service Operator.

Consistent with healthcare record management practice, clinical documents within the *PCEHR* are not to be edited or deleted. Any changes to records will require a new version of the clinical document to be issued.[96] The *PCEHR* system treats the originating source system as the 'source of truth' and holder of the primary copy of the information.[97] If a clinical document contains incorrect information, there is a correction process that can be implemented; however the level of computer skills needed by a consumer in order to access this function is quite sophisticated and may be out of reach for some groups such as elderly patients or those patients who do not own a computer.[98] Consequently a clinical document that has been 'effectively removed' from an individual's *PCEHR* is not deleted.[99]

The *PCEHR* permits authorised users to access, download and/or print any clinical documents. The information can also be downloaded to the organisation's local electronic health record system. It is assumed by NEHTA that the downloading and/or printing of *PCEHR* information will be in compliance with present medico-legal integrity requirements.[100] Once information has been downloaded and/or printed it becomes subject to the organisation's local health information management policies and laws applicable to the organisation.[101]

---

[96] NEHTA, *Concepts of Operations*, above n19: at 34-35.

[97] Ibid 47.

[98] NEHTA Clinical Lead, Dr Kean-Seng Lim, *The PCEHR and the General Practitioner* (3 April 2013): at 10.

[99] NEHTA, *Concepts of Operations*, above n19: at 48.

[100] NEHTA, *Concepts of Operations*, above n19.

[101] NEHTA, *Concepts of Operations*, above n19, 48-49.

The *PCEHR* is primarily about *shared* information and as a result is populated by sites dealing with shared health summaries, event summaries, discharge summaries, specialist letters, referrals, prescribing and dispensing information amongst other things.[102] One source of *PCEHR* documentation is information currently held by Medicare. There is continuing controversy as to why Medicare information held separately will be included in *PCEHR*. For its part, NEHTA states that there is an opportunity to leverage the information collected by the Department of Human Services Medicare program.[103] It is acknowledged by NEHTA that while this information lacks the clinical relevance and richness of other information sources, such as discharge summaries, included with patient consent,[104] the Medicare information provides a longitudinal source of information about an individual's healthcare events.[105] However, given that healthcare identifiers are mandatory and will include Medicare information that has already been collected before the system commenced, it is hard to imagine how consent requirements will operate in relation to health information collection and use.

The provision of this level of information will mean that the *PCEHR* will be a very rich source of personal data containing not just health information but also specific activity information (such as individual, family members and health provider

---

[102] NEHTA, *Concepts of Operations*, above n19 [for full details of what is included in the *PCEHR*]: at 50-60.

[103] Medicare Australia operates 2 data information systems – the CDMS is the Consumer Directory Maintenance System and the PDS is the Provider Directory System; see also chapter 2, fn33, p47.

[104] NEHTA, *Concepts of Operations*, above n19, there is no definition or explanation of the meaning of 'with consent' in the NEHTA, *Concepts of Operations*, above n19: at 55.

[105] NEHTA, *Concepts of Operations*, above n19.

information).[106] It is also envisaged that the *PCEHR* will provide very detailed information about individuals that may also be of interest to organisations such as national security and law enforcement agencies on the basis of national security issues. The thesis argues that there will be a temptation (known as 'drag-net fishing')[107] to use this rich source of information for hungry health and non- health organisations in search of information (including identified and yet to be identified 'healthcare providers'[108]) and that the temptation to collect information is real and presents a threat to individual privacy rights.[109] This point is discussed further in chapter 6 in relation to e-health governance issues.[110]

NEHTA envisaged that a combination of legislation, technical and governance safeguards would be capable of preventing unauthorised and inappropriate access and use of healthcare information.[111] A vital feature of the *PCEHR* system security and privacy is an online audit record available to individual *PCEHR* users. Additional safeguards underpinning the *PCEHR* system include: technical security measures, training, effective and transparent governance arrangements, legal protections and penalties, and regulatory oversight.[112]

---

[106] See Daniel Solove, *The Digital Person* (New York University Press, 2004) [where Solove argues that the collection of health and other personal information will allow individual 'dossiers' to be created]: at 3; see also Daniel Solove, Marc Rotenberg and Paul Schwartz, *Privacy, Information, and Technology* (Aspen Publication,2006); David Brin, *The Transparent Society* (Perseus Books, 1998): at 32.

[107] Daniel Solove, *The Digital Person*, above n106.

[108] See chapter 5, pp178-182 and chapter 6, pp231-234.

[109] See chapter 5, pp178-182 for discussion on 'function creep' and 'data mining'.

[110] See chapter 6, pp231-234.

[111] NEHTA, *Concepts of Operations*, above n19: at 61.

[112] NEHTA, *Concepts of Operations*, above n19.

As later highlighted in chapter 6, the main problem with the stated safeguard system is that the *PCEHR* system's governance arrangements, regulatory framework, including complaints management and sanctions are still in the process of development and are not fully operational despite the July 2012 *PCEHR* commencement date having come and gone.[113] This lack of long-term governance and complaints arrangements has been strongly criticised by groups such as the Community Health Forum (CHF) as being unacceptable for the community.[114]

Progressing forward from 2005-14 the implementation and roll out of the *PCEHR* by NEHTA continues with allocation of individual-provider healthcare identifiers numbers and enactment of *Healthcare Identifiers Act 2010* (Cth) and *Personally Controlled Electronic Health Record Act 2012* (Cth). However since late 2013, which saw a change of federal Government, the *PCEHR* and e-health system implementation has been under review by the new Government.[115]

Further 2013-14 NEHTA roll out initiatives include:

- Upgrades to consumer registration process;
- Introduction of the first four ePIP requirements. Medicare Locals continue to support practices with ePIP requirements and e-health registration workshop packages;
- New ePIP requirements for General Practices.
- PCEHR compliant software now represents 90% of GP software market and can be downloaded;
- Promotion of e-health consumer registration by direct mailing to general public and local advertising;
- The assisted registration tool is now available on the e-health website;
- In readiness for increased capability all primary healthcare providers, including practice nurses and allied healthcare providers are encouraged to register for a Healthcare Identifier

---

[113] See Kate Newton, 'PCEHR Deadline Chaos' *Australian Doctor* (Australia), 25 January 2013, 1; see also Danielle Cesta, 'More E-Health Tech Drama' *Medical Observer* (Australia), 12 April 2013, 11.

[114] See Consumer Health Forum (CHF), *CHF Response to the Concept of Operations Relating to the Introduction of a Personally Controlled Electronic Health Record System* (October 2011): at 11-12.

[115] See *Royle Review*, above n56 [This commissioned review is outlined and discussed in chapter 7, pp250-255].

number. Accredited Practicing Dieticians and Accredited Nutritionists need only supply the HI Service with proof of membership in order to evidence their identity;

- New e-health record link for your website.[116]

Alongside the physical development and implementation of e-health architectural and design schemes such as healthcare identifiers and *PCEHR* programs, the increasingly thorny issue of privacy, security law and e-health system governance continues to dominate the federal Government's health reform agenda.

V. CONCLUSION

Much has been achieved by different Australian Governments over the last twenty and more years in the e-health area. The narrative outline of introduction of a new electronic health regime analysis in Australia started with the recognition by government that in a modern economic and information digital era, electronic health records would represent the best solution to ensuring ongoing healthcare for all Australian citizens in an increasingly globalised world. Once this political decision had been reached, research, development, implementation and roll-out of the *PCEHR* and e-health Systems was initiated. Considerable financial support via federal funding was also made available, as well as federal/State/Territory cooperation in order to progress the e-health vision into a reality.[117] Particularly in the past ten years

---

[116] NEHTA, *Roll out of the PCEHR* (February 2013 Bulletin); see Fact Sheet homepage http://www.nehta.gov.au/ehealth-implementation/roll-out-pcehr (viewed on 16/9/2012); NEHTA, *Next Steps After You Receive Identity Verification Code* (IVC) (2013) http://e-health.gov.au/internet/ehealth/publishing.nsf/Content/brochure-ivc (viewed on 23/7/2013); see also NEHTA, *E-Health Fact Sheet – Prescribed and Dispensed Medication* (2013) 'Your Medications Online' NEHTA Homepage (online) Fact Sheet; Chloe Herrick, 'Federal Government Sheds Light on Next Round of E-Health Record Funding' *Computerworld* (Australia), 7 October 2011, 2.

[117] See, for example, federal *Budget* 2010-2012 (committed $466.7 million over 2 years); federal *Budget* 2012-2014 (committed $233.7 million over 3 years); federal *Budget* 2014-2015 (committed $140.6 million for 1 year). See also COAG, Australian Health Ministers' Conference, *Joint Communique,* above n6 [Where it is recognised that new health council a vital link to future health information management in Australia].

(since NEHTA) the *PCEHR* has gone from a 'virtual' concept to a physical one, even though there is still much to do in relation to system governance and privacy protection.[118]

However further political and economic change is on the horizon following the September 2013 change of federal Government in Australia — and the full impact of its health, *PCEHR* and e-health policy is yet to be fully revealed and its impact felt.[119] Even so, it can be predicted that this political change will alter the ongoing *story* of health, *EPR*, e-health and privacy, since there are already some early disturbing trends emerging.[120] The Abbott Coalition Liberal Government is committed to re-evaluating and rationalising current healthcare spending and policy in Australia.[121] The Coalition Liberal Government is wedded to progressing neoliberal pluralistic ideals of 'decentralisation', privatisation and commercialisation of health' and globalisation — a focus which continues to challenge the very foundations and future of Australian public healthcare delivery.[122] This policy shift is evidenced in the 2013-14 federal *Budget* released in May 2014.

---

[118] See NEHTA, *Strategic Plan Refresh 2011/2012* (2011). The NEHTA's strategic plan describes the COAG funded milestones achieved to date, the work planned to progress the key e-health foundations and initiatives for the remaining period of NEHTA's current COAG funding, the targets and activities required to deliver components of the *PCEHR*, and NEHTA's role in accelerating the adoption and further progression of e-health in Australia into the future: at 2.

[119] Federal Australian Government elections held September 2013.

[120] See *Royle Review*, above n56; see also chapter 6: at pp190-203. The review makes 38 recommendations to the federal Government on *PCEHR* governance such as dissolving NEHTA (Rec. 1): at 16-18; see also Federal Coalition Government, *The Coalition's Policy for E-Government and the Digital Economy* (September 2013).

[121] See Australian Government, federal *Budget* 2014-2015 *Health* (13 May 2014). See, for example, the case for change - the introduction of a new Medicare Safety Net (similar to the safety net used in *Fair Work Act* 2009): at 3, 9-10; a new federal *Budget* 2015 is now released (after completion of the thesis).

[122] See federal *Budget* 2013-14; see also Ben Grubb, 'Abbott Government 'Uncomfortable with Freedom of Information' *Sydney Morning Herald* (Australia), 14 May 2014, 28; Andrew Bracey, 'Rich Should Cough Up: Dutton' *Medical Observer* (Australia), 28 February 2014, 1.

The following chapter 3 continues to focus upon and analyse the changing political, social and economic environment that impact on Australian healthcare delivery systems. It does this by providing a detailed historical and theoretical analysis of technology in the modern knowledge and information driven age. It also explores the proposition that healthcare privacy is compromised by developing technologies: a situation which if confirmed presents further evidence that an *Independent Council* might contribute to a feasible solution in order to address this looming imbalance.

CHAPTER 3

TECHNOLOGY AND THE NEW ELECTRONIC HEALTHCARE REGIME

This chapter details the nature and scale of the challenges to privacy and democratic policy-making posed by the technologies implicated in an electronic healthcare regime. It provides a deeper conceptual analysis of the transformational power of technology on lives by exploring its impact on society, tracing its historical beginnings through to its present day conception. It also highlights concerns about electronic healthcare privacy and its potential capacity to subsume individual and community rights in favour of collective government and economic interests. Finally, the chapter argues that there is a need to reconsider our present concept of both technology and privacy in light of new forces that impact on contemporary healthcare technology privacy debate.

I. RISE OF COMPUTER AND INFORMATION TECHNOLOGY

Developments in technologies continue to influence the debate about privacy and the evolution of information privacy laws in Australia.[1] As early as 1890 in their famous article on "The Right to Privacy", Warren and Brandeis identified the social impact

[1] See Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era*: Discussion Paper 80 (March 2014): at 21; see also ALRC, *Serious Invasions of Privacy in the Digital Era*: Issues Paper 43 (October 2013).

that new photographic, printing and media technologies had on individual privacy rights and articulated the need for a legal response to new technologies.[2] Although historically distinct, Warren and Brandeis' anxieties about advancing technology and privacy concerns still strongly resonate in the 21st century, as people continue to grapple with legal and ethical implications of rapidly advancing technologies and its impact on individual privacy rights.[3]

The evolution of technology, particularly computer and information technology has contributed to social, economic and political theoretical discourse including healthcare technology dialogue. Every culture must negotiate with technology and the uses made by technology are largely determined by the structure of technology itself – that is function follows form:

> Once technology is admitted, it plays out its hand; it does what it is designed to do. Our task is to understand what that design is – that is to say when we admit a new technology to the culture, we must do so with our eyes wide open.[4]

New technologies give rise to new definitions of old terms, as well as introduce new terms and words and that this happens without being fully conscious of it.[5] The language of computers and technology is now part of our everyday language, with words such as Microsoft, Amazon, Facebook, Twitter and Google almost universally understood.[6] However the ultimate power of technology is that it eliminates alternatives to itself, not by making it illegal, nor immoral, or even unpopular but by

---

[2] See Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

[3] Australian Government, National E-Health Transition Authority (NEHTA), *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* (September 2011): at 11.

[4] See Neil Postman, *Technopoly: The Surrender of Culture to Technology* (Vintage Book, 1993) 7.

[5] Ibid 8.

[6] See Cheryl Tang, *Microsoft First Generation* (John Wiley & Sons, 2000) 2.

making them invisible and therefore irrelevant.[7] It does this by redefining what is meant by art, religion, politics, family, health, truth, education, intelligence, surveillance and privacy, so that definitions of such terms fit technology's new requirement.[8] Technology lays the foundation of human beings as objects and is capable of depriving people of the social, political, historical, metaphysical, logical or spiritual bases for what is beyond belief.[9]

The information age is also known as the computer era. The revolutionary aspect of this era is the freedom and ability of governments, businesses and individuals to transfer information and gain instant access to knowledge. This ability is linked to the digital revolution and implies a shift from the traditional notion of industry that the industrial revolution brought through industrialisation to an economy founded on the gathering and manipulation of ideas.[10] What has made this transition from an industrialised world to an information economy possible is the ability to capitalise on advances in computer microminiaturisation, the advent of personal computer in the late 1970s and internet developments in the 1990s bringing the development of technology to a critical point.[11]

---

[7] See Neil Postman, *Technopoly*, above n4.

[8] Ibid 48.

[9] Ibid.

[10] Don Ihde, *Philosophy of Technology* (Paragon House, 1993) 45.

[11] Michael Hobart and Zachary Schiffman, *Information Ages: Literacy, Numeracy, and the Computer Revolution* (John Hopkins University Press, 2000); see generally Christopher Arup, *Innovation, Policy and Law: Australia and the International High Technology Economy* (Cambridge University Press, 1993) [Arup examines the nature of innovation and the transformation of the economy, influencing the distribution of power and wealth]; see also Brian Galligan, Winsome Roberts and Gabriella Trifiletti, *Australians and Globalisation: The Experience of Two Centuries* (Cambridge University Press, 2001).

The advantages for government and business interests in communication technology is that digital technology enables rapid, cheap and efficient collection, storage and retrieval of personal information instantly available from all corners of the globe. Progression of technologies such as computers, cyber-space, internet, cloud computing and social networking has developed at a phenomenal rate, often resulting in society adjusting to the demands of technology rather than controlling the process.

The significance of the development of IT over the last few decades relates to the functionality of 'tools' such as computers and overall capacity and availability. The 'seduction' and rising popularity of computers (and recently smart phones and tablets) has meant that there is an ever-increasing capacity to generate, link and store more and more information.[12] This may occur even to the detriment of an individual's right to privacy. As Scott McNealy, CEO, Sun Microsystems, Inc. states, 'You already have zero privacy. Get over it'.[13]

It is within this fast moving dynamic digital information economy environment that healthcare *EPR* and e-health systems will be located. It can be envisaged that the emergence of electronic health regimes represents a crucial shift away from traditional healthcare delivery thinking in that it physically and symbolically changes the expectations and mindset that people hold about their health experience. For instance,

---

[12] See Hobart and Schiffman, *Information Ages*, above n11; see Roger Magnusson, "Data Linkage, Health, Research and Privacy: Regulating Data Flows in Australia's Health Information System" (2002) 24 *Sydney Law Review* 5; see also Danuta Mendelson, "Health*Connect* and the Duty of Care: A Dilemma for Medical Practitioners" (2004) 12 *Journal of Law and Medicine* 69. Both Magnusson and Mendelson recognise the rising popularity of computers and their ever-increasing ability to generate, link and store information such as healthcare information.

[13] Scott McNealy, CEO, Sun Microsystems, Inc. (March 1999) quoted in Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press, 2003): at 50.

the introduction of healthcare identifier numbers in Australia opens a major gap between the physical and the 'virtual' identity. This virtual digital identity affects how consumers, healthcare providers and other stakeholders view healthcare delivery expectations and privacy rights in the future.[14]

A. *Computer technology*

Computer technology has undergone rapid significant changes in a relatively short period of time.[15] The evolutionary leap of computers from simple utility calculating machines to hi tech computation tools capable of both information collection and intrusive data analysis is evident in the modern information era. As computers become more than 'tools' of utility and convenience in our community we need to further understand the long-term outcomes of our modern technology.[16] The adoption by the Australian Government of *EPR* and e-health technology is premised on the continuing progress and availability of 'networking' communication technology and its tools such as computers, tablets, smart phones and internet systems.[17]

---

[14] See Tal Zarsky, "Mine Your Business!": Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion" (2003) 5 *Yale Journal of Law and Technology* 1; see also Jaron Lanier, *Who Owns the Future* (Penguin Books, 2013); Jaron Lanier, *You Are Not A Gadget* (Alfred A. Knopf, 2010) [Lanier offers a view of the revolutionary changes since Silicon Valley and the World Wide Web (WWW) has and will bring to commerce and culture]. See also Department of Parliamentary Services (Cth), Rhonda Jolly, *Healthcare Identifiers Bill 2010 Bills Digest*, No 116 of 2010, 24 February 2010.

[15] See Don Ihde, *Philosophy of Technology*, above n10 [Don Ihde identifies the different phases of computer development, which according to Ihde broadly reflect other advances involving evolution of mainframe, minicomputers and microcomputers]. Computer technology development generally refers to 3 distinct generations of computer technology – the first generation (1950-1958); the second generation (1959-1964); and the third generation (1964 onwards): at 45-46.

[16] See Evgeny Morozov, "The Real Privacy Problem" (November/December 2013) 116(6) *MIT Technology Review* 32.

[17] See, for example, Australian Government, Council of Australian Government (COAG), *Joint Communique: New Council a Vital Link to Future Health Information Management Australia* (28 November

B *Internet and Cyber-Space*

Alongside advancing computer technology the growth of the internet, its connectivity and 'networking' ability has contributed to the advancement of IT as a dominant communication player. A major feature of the Internet is its 'end-to-end design and instantaneous transnational dimension'.[18] Once the internet world is entered, users enter a transnational state that flows beyond the normal static borders of any one state resulting in the movement of information through space in most instances is rapid, cheap and ubiquitous.[19] According to Perritt, 'the internet has firmly established itself as the model for global information.'[20]

The High Court of Australia has described the internet and cyber-space as a 'decentralised, self-maintained telecommunication network. It is made up of interlinking small networks from all parts of the world.'[21] It has also been described as 'an international network of interconnected computers…which now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world.'[22]

2003); Australian Government, *A National Health and Hospitals Network for Australia's Future Health Strategy* (2010); Deloitte, National E-Health and Information Principal Committee, *National E-Health Strategy* (30 September, 2008).

[18] Brian Fitzgerald, Anne Fitzgerald, Gaye Middelton, Eugene Clark and Yee Fen Lim, *Internet and E-Commerce Law, Business and Policy* (Thomas Reuters, 2011) 6-7.

[19] Fitzgerald, Fitzgerald, Middelton, Clark and Lim, *Internet and E-Commerce Law*, above n18: at 7.

[20] See H Perritt, 'Jurisdiction in Cyberspace: The Role of the Intermediaries' in Brian Fitzgerald and Anne Fitzgerald, *Cyberlaw* (LexisNexis, 2002): at 122-123; see Fitzgerald, et al, *Internet and E-Commerce Law*, above n18: at 12-13.

[21] *Dow Jones v Gutnick* [2002] HCA 56 per Kirby J: at Para 80.

[22] *Reno v American Civil Liberties Union* (1997) 521 US 844.

Cyber-space is an illusion because it has no physical presence. Yet its users visit it, send messages and transact business through it. Electrical optical and magnetic forces with storage facilities allow users to carry out steps that produce a result in real space.[23] As noted by John Perry Barlow, Co-Founder, Electronic Frontier Foundation, Cyber-space is the new frontier for gathering personal information and its power has only begun to be exploited:

> Cyberspace, the new home of mind…We have no elected government, nor are we likely to have one…I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral to rule us nor do you possess any methods of enforcement we have true reason to fear… Cyberspace does not lie within your boundaries…Your legal concerns of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here.[24]

The importance of the internet in the new electronic healthcare regime is that it provides the essential medium in which *EPR* information data can be collected, stored, accessed and *shared* in the digital environment.

C. *Cloud Computing*

A further technological advancement that impact of healthcare delivery and privacy protection is Cloud computing.[25] What Cloud computing does is link computers in a

---

[23] See Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press, 2009): at 12; see generally Olujoke Akindemowo, *Information Technology Law in Australia* (Thomas Reuters, 1999).

[24] See John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) cited in Alan Davidson, *The Law of Electronic Commerce*, above n23: at 14.

[25] See Fitzgerald, et al, *Internet and E-Commerce Law*, above n18 describes 'Cloud Computing' and its impact on consumers and businesses, he identifies that government is already using this type of technology system as a way of cutting administration costs. However, the majority of individuals may not be fully aware of nor appreciate this situation: at 12-13; see also Caroline Klein, "Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care" (2011) 39 *Journal of American Academic Psychiatry Law* 39; see also Australian Institute of Criminology, Raymond Kim-Kwang Choo, *Cloud Computing: Challenges and Future Directions* (October 2010); Australian Government, Department of Finance and Deregulation, Government 2.0 Taskforce (Chair Nicolas Gruen), *Engage – Getting on with Government 2.0* (December 2009).

networked grid, thus enabling on-demand access to a shared pool of computing resources that are readily available with minimal management effort or service provider interaction.[26] Cloud computing involves storing digital content on servers maintained by large technology companies, instead of on a local hard drive. This enables consumers and businesses to have documents and programs delivered directly from a communications provider, rather than having to run desktop computers. Users can access data and software stored on the grid from any PC, laptop or mobile device, anywhere in the world.[27]

Although Cloud computing offers real benefits for consumers, business and governments it also introduces risks, notably threats to the privacy and security of stored data.[28] This is because the increasing use of Cloud computing with greater amounts of data being collected and stored for longer periods of time raises issues about privacy and security of remotely stored and/or offshore data. The absence of effective legislative protection of privacy and the international cooperation to ensure the security of data that crosses national borders also contributes to privacy and security concerns. Although Cloud computing was not specifically considered by the ALRC in its 2008 review of privacy law, the Federal Government has recognised its

[26] L Martin, Australian Government, *Awareness, Trust and Security to Shape Government Cloud Adoption: A White Paper* (April 2010).

[27] J Bajkowski, 'Future is Fixed, Thank God' *Australian Financial Review* (Australia), 11 November 2010, 66.

[28] See NEHTA, *The Best and Worst of Cloud Contracts* (8 March 2013).

increasing influence and identified good practice guidelines on privacy and security as an important component of its Cloud Framework.[29]

D. *Social Networking*

Since mid-2000s there has been a rapid uptake of internet-connected smartphones (mobile phones with embedded computer power) and tablet devices such as iPad, iPod, Galaxy Tablets. The widespread adoption of this type of technology, which runs applications (apps) in addition to the kind of software programs loaded onto computers, has brought about a fundamental shift in user experience of the internet.[30]

This situation has resulted in a significant increase, especially in the 15-17 year age group of the number of smartphone owners, who routinely use the Internet, send and receive email and communicate using programs such as Instagram.[31] Social networking sites like YouTube provide great entertainment; opportunities as well as many benefits. But equally there can be downsides to these opportunities and benefits.[32] The YouTube story of the Korean 'dog poop girl' provides a sobering

---

[29] Australian Government, Department of Finance and Deregulation, *Cloud Computing Strategic Direction Paper – Draft Consultation* (January 2011) [This Strategic Direction Paper considered Cloud computing and its possible impact on society was considered by the Australian Government].

[30] See Fitzgerald, et al, *Internet and E-Commerce Law*, above n18: at 10.

[31] Australian Government, Australian Bureau of Statistics, *8153.0 – Internet Activity, Australia June 2014* 12,483,000 internet subscribers in Australia at the end of June 2014 representing an increase of 1% from June 2013; *Patterns of Home Internet Use* 2014, Online banking 72%, Social networking 66%, listening to music, watching video 58%, accessing Government services 58%; *Personal Internet Use* 2012-13, 83% of persons were internet users. The 15-17 age group had the highest proportion of internet use 97% with the lowest being 65 and over age group 46%; *Australian Population Clock* as on 23 January 2015 23,720,067 people; see *Australian Historical Statistic's,* 2014, 3105.065.001 (2014) sets out statistics of geographic, health status and other important statistical material such as Australian ageing and migration trends. See also ALRC, *Serious Invasions of Privacy in the Digital Era*: Issues Paper 43 (October 2013); ALRC, *Review of Privacy:* Issues Paper 31 (October 2006): at 513-544 (Developing Technology).

[32] See, for example, 'dog poop girl' (viewed on June 2005) (online) see Youtube; see also Daniel Solove, *The Future of Reputation* (Yale University Press, 2007) [when poop goes primetime]: at 1-4; see also Hassan Masum and Mark Tovey (eds), *The Reputation Society: How Online Opinions Are Reshaping the Offline World* (The MIT Press, 2011); Daniel Solove, *Nothing to Hide: The False Tradeoff Between Privacy*

example of the power of information technology and its ability to destroy reputations and lives across international boundaries.[33]

E. *Surveillance*

The ensuing 'war on terror' resulted from the attack on the World Trade Centre in New York and later the bombings in Bali and London.[34] This term 'war on terror' was coined by the President of the United States George W Bush.[35] From 2001 western societies have experienced an increase in legal measures and national security concerns, which has further accelerated the development and use of surveillance technology to a new level in all areas of citizens' lives.[36] These include ensuring that 'terrorist acts' are established as serious criminal offences in domestic laws and regulations.[37]

---

and Security (Yale University Press, 2011); Stuart Biegel, *Beyond Our Control,* above n13 ; Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, 2001).

[33] See Daniel Solove, *The Future of Reputation*, above n32: at 1-4; Jonathan Krim, 'Subway Fracus Escalates into Test of Internet's Power to Shame' *Washington Post* (United States), 7 July 2005, 1; Daniel Solove, *The Digital Person* (New York University, 2004); see also Masum and Toovey, *The Reputation Society*, above n32.

[34] Helen Duffy, *The War on Terror and the Framework of International Law* (Cambridge University Press, 2005) [The World Trade Centre was attacked on 11 September 2001; see also Bali terrorist bomb attack in 2003, the London terrorist bomb attack in 2005]; see also December 2014, attack by gunman at Lindt café, Martin Place, Sydney, Australia.

[35] Helen Duffy, *The 'War on Terror'*, above n34: at 17.

[36] See Jeffery Rosen, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror" (2004) 46 *Arizona Law Review* 607; see Jeffery Rosen, *The Naked Crowd: Reclaiming Security and Freedom in* an *Anxious Age* (Random House, 2004); see also Jeffery Rosen, *The Unwanted Gaze,* above n32. .

[37] See Christopher Michaelson, "Antiterrorism Legislation in Australia: A Proportionate Response to the Terrorist Threat?" in *Studies in Conflict and Terrorism* (Routledge, 2005); see *European Council Framework on Combating Terrorism*, 13 June 2002, [2000] OJL 164/3 33, 34, 37, 132, 350; Preamble, *Guidelines on Human Rights and the Fight against Terrorism*, adopted by the Committee of Ministers of the Council of Europe on 11 July 2002; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism *Act* (*USA Patriot Act*) of 2001, Pub. L. No. 107-56, 115 Stat. 272; *Crimes Act 1914* (Cth); *Criminal Code Act 1995* (Cth) "terrorist act" defined in Criminal Code subsection 100.1(1), Part 5.3 or 5.5; see also *Charter of the United Nations Act 1945*.

As a culture obsessed with surveillance of people often privacy rights are overridden by perceived needs of national security and law enforcement agencies (both public and private). For instance, this is evidenced by the number of CCTV cameras now found throughout the UK, which now averages one camera for every four citizens in London and every 34 people in the country.[38]

F. *Biometrics*

The growing need for surveillance at a national and international level is further supported by advances in technology such as biometrics and DNA-Profiling. Biometrics is the study of methods for uniquely identifying humans based upon one or more intrinsic physical or behavioural traits. In information technology, biometric authentication refers to technologies that measure and analyse human physical and behavioural characteristics for identification purposes. This includes fingerprints, eye retinas and irises, facial patterns and hand measurement, while examples of behavioural traits include electronic signature, gait and typing patterns.[39]

---

[38] See Olivia Goldhill, 'Britons Embrace CCTV Cameras' *The Telegraph* (UK), 6 November 2014, 1 [London Councils London has the highest number of CCTV cameras in the world (approximately 7,000 cameras)]; see also Paul Lewis, 'You're Being Watched: There's One CCTV Camera for Every 32 People in UK'], *The Guardian* (UK), 3 March 2011 (online); see *Privacy Act 1988* (Cth) s6F; *Freedom of Information Act 1982* (Cth) s43(1) [provides that a document is exempt if its disclosure under the Act would disclose one or more prohibited situations outlined in the Act]; *Healthcare Identifiers Act 2010* (Cth) s5 and *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR) s16 [which specifically exclude operation of the Act in relation to defence forces and national security requirements]. The 'System Operator' (Medicare) is obliged to make available to authorised national security bodies (without the knowledge or consent of the person to whom the file relates.

[39] See ALRC, *Review of Australian Privacy Law*: Discussion Paper 72 (December 2007) [this discussion paper describes 'biometric technologies as enabling the identification of unique behavioural and physical attributes of people to be used for identification and authentication purpose']: at 330. A typical biometric device is finger and iris scanners. Biometric technologies have existed for decades. However, with the increase of globalisation and developments in technology the use of biometric technologies is on the rise because of the need to identify individuals and manage security threats such as terrorism: at 330. The ALRC, Discussion Paper 72 [distinguishes between 'biometric technologies from DNA-based technologies - observing that DNA- based technologies require actual physical samples to be taken from a person, as opposed to the taking of an image or scan of the person' (biometrics)]. This

The significance of biometric advancements is that identification and authentication is foundational (key) to the operation of the new electronic healthcare regime.[40] The 'right information about the right person' is the mantra often quoted by the Australian Government in relation to *EPR* development and implementation.[41] This is because it is easy to assume another person's identity or hide your true identity using information technology such as internet. The possibility of cybercrime such as identity fraud and identity theft using technology is a major problem not just for healthcare privacy and security but also individuals and business operations.[42]

II. LIMITATIONS OF RAPIDLY DEVELOPING TECHNOLOGY – SECURITY AND PRIVACY

A. *Security*

Information security is high on the priority and anxiety list for all healthcare stakeholders, particularly consumers.[43] This is due to the nature of electronic data creation and collection and the ease in which it can be collected, changes, accessed and stolen all contributing to ongoing privacy issues. A major challenge for the creators of *EPR* is security in relation to unauthorised access, identity theft, control of

---

physical sample process raises a number of privacy issues including possibilities of discrimination: at 333-334. For example, see ALRC and the Australian Health Ethics Committee (AHEC), *Essentially Yours: The Protection of Human Genetic Information in Australia* (2003). This report was a product of a two-year inquiry into the legal and ethical issues surrounding human genetic information. See also, Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, 2002). Laurie provides a detailed analysis of the medico-legal and ethical issues in this area of the law; see Australian Government, ALRC, *Serious Invasions of Privacy in the Digital Era*: Discussion Paper 80, above n1: at 40.

[40] NEHTA, *Concepts of Operations,* above n3: at 61.

[41] Ibid.

[42] Peter Grabosky, Russell Smith and Gillian Dempsey, *Electronic Theft Unlawful Acquisition in Cyberspace* (Cambridge University Press, 2001); see also Daniel Solove, *Nothing to Hide,* above n32.

[43] ALRC, Discussion Paper 72, above n39: at 1503.

information and unsanctioned data changes. Cybercrime and computer security breaches represent a worrying and rising problem in technology. Statistically most cybercrime and security breaches occur within particular organisations by current or ex members of those organisations; although outside people such as hackers and crackers contribute significantly to the problem.[44] There are no system or software programs that can guarantee that digital data is 100% protected and secure from unauthorised or criminal elements. There are controls that can be used to add protection to the system or encode information itself, but none of this software is fool proof against determined hackers.

At present it can be asserted that with the main government regulatory focus on *EPR* cyber security, rather than local data security many smaller healthcare entities (i.e. medical centres, sole practices) remain vulnerable to computer hackers and international criminals because their management and administrative systems are not inadequately protected against attacks. This situation is evidenced by the recent rise of organised criminal cyber — extortion attacks on local computer systems containing business records (as well as sensitive patient information) in Queensland.[45]

Despite the push by government and professional associations encouraging upgraded business security software and technology measures compliance at the

---

[44] See Russell Smith, Peter Grabosky and Gregor Urbas, *Cyber Criminals on Trial* (Cambridge University Press, 2004) 9.

[45] See Smith, Grabosky and Urbas, *Cyber Criminals on Trial*, above n44: at 5; see Kate Newton, 'GP Clinic Stands Firm Against Extortion Attempt from Hackers' *Australian Doctor* (Australia), 18 January 2013, 4; see also Neil Bramwell, 'Privacy Minefield' *Medical Observer* (Australia), 11 April 2014, 14; see, for example, David Watkins, 'Sony Apologies for PlayStation Privacy Breach and Boosts Security' *Herald Sun* (Australia), 2 May 2011 (online) http://www.heraldsun.com.au/news/world/sony-apologies-for-playstation-privacy-breach (viewed on 1/8/2011).

medical coalface is expected but voluntary. The e-health system allows and indeed caters for healthcare providers and associated organisations to upload patient medical records from the *PCEHR* it seems only logical that if digital records are kept locally as electronic records there must be clear and strong regulations to force all providers — whether business big or small — to install and technically maintain more than *adequate* computer security protection of all records.

EPR and e-health computer protection and security consists of a combination of passwords, review processes, audit trails, consumer access to one's own records and other security measures would prevent unauthorised people from accessing and browsing through records.[46] As a national network it was recognised in 2001 at the beginning by Health*Connect* that the rules and measures relating to privacy and e-security would need to be the same across Australia. The development of security is recognised as a fundamental requirement for an organisation's survival in the changing, frenetic world of electronic information and commerce.[47] The meaning of the term e-security is wide ranging and covers the protection of online electronic data as well as the prevention of impairment to any system that provides communication functionality. Vulnerability to greater risks by organisations in relation to unauthorised access, misuse, modification and misappropriation of data is significant.

---

[46] NEHTA, *Concepts of Operations,* above n3: at 61-73; The Royal Australian College of General Practitioners (RACGPs), *Computer and Information Security Standards* (October 2011) http://www.racgp.org.au/download/Documents/Standards/2011computerinformationse (viewed on 15/4/2013) 16; Health*Connect*, Health*Connect*, *Consent and Electronic Health Records – A Discussion Paper* (July 2002): at 12-13.

[47] Leif Gamertsfelder, *E-Security* (Thomas Reuters, 2002) 3.

There can be enormous costs to an organisation's reputation, image and finances when its network security is compromised.

B. *Privacy protection*

The *PCEHR* system recognises that privacy is of critical importance.[48] Successful delivery of privacy will ensure ongoing confidence and trust in the new electronic healthcare regime and increase its uptake by consumers and healthcare providers. It is acknowledged by the National E-Health Transition Authority (NEHTA) that there is no single solution to addressing privacy issues.[49] The protection of privacy is a priority for the *PCEHR* design, using a combination of technical, policy, governance and legislative safeguards.

As later explained, the thesis proposal for the introduction of a *Council* would ensure that individual privacy protection remains a priority for the government in light of rapid developments in intrusive technologies.

III. OVERVIEW OF THE THEORETICAL DEVELOPMENT OF TECHNOLOGY

There are three major broad theories of technology that require consideration when examining the impact of *EPR* technology on issues of privacy and security. The first concept can be termed the instrumental theory the second is the substantive theory and the third is 'critical theory'. Instrumental theory represents the dominant view

[48] Australian Government, National E-Health Transition Authority (NEHTA), *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System* (September 2011) 61.
[49] Ibid.

taken by government and policy sciences and treats technology as subservient to values in other social spheres, for example, politics and culture. On the other hand substantive theory attributes to technology an autonomous force that overrides all traditional or competing values. Substantive theory claims that what the very employment of technology does to humanity and nature is far more consequential than its ostensible goals.[50] Critical theory for its part rejects the concept of neutrality of technology, arguing its political rationality.

Instrumental theory is the most widely accepted view of technology, supporting the notion that technologies are 'tools' that are ready to serve the purpose of their users. This theory believes that technology is *neutral*, without valuable content of its own. The theory posits four main 'neutrality' arguments. Firstly, that technology represents pure instrumentality and it is thus indifferent to the variety of ends it can be employed to achieve. Secondly, the transfer of technology in a modern world is indifferent to politics, especially in relation to capitalist and socialists societies. Thirdly the socio-political neutrality of technology is attributed to its 'rational' character and the universality of the truth it embodies. Finally, the universality of technology also means that the same standards of measurements can be applied in different settings. Thus technology is routinely said to increase the productivity of labour in different countries, different eras and different civilisations.

[50] See Andrew Feenberg, *Transforming Technology: A Critical Theory Revisited* (books.google.com. 2002); see also Andrew Feenberg, *Critical Theory of Technology* (Oxford University Press, 1991) 5-6; Richard Coyne, *Designing Information Technology in the Postmodern Age: From Method to Metaphor* (The MIT Press, 1995).

Therefore technologies are neutral because they stand essentially under the very same norm of efficiency in any and every context.[51]

Given the above understanding of technology, it is logical to argue that there should be unreserved commitment to its employment. Nevertheless, there are some objections to this stance, including certain deference to moral values. A case in point is reproductive technology. Andrew Feenberg states that even if one believes that abortion and test tube babies are valuable in themselves and technically available, one can only judge these actions in terms of efficiency and respect for beliefs such as the sacredness of life.[52]

The instrumental approach places 'trade-off' at the centre of the debate. The belief that 'you cannot optimise two variables' is the fundamental law of the theory. What this implies is that there is a price for the achievement of environmental, ethical or religious goals and that price must be paid in reduced efficiency. Based upon this account the technical sphere can be limited by nontechnical values but cannot be transformed by them.[53]

Substantive theory denies that technology is neutral. The main exponents of this theory are Jacques Ellul and Martin Heidegger, who believe that technology constitutes a new type of cultural system that restructures the entire social world as

---

[51] Andrew Feenberg, *Critical Theory of Technology*, above n50: at 6; Andrew Feenberg, *Transforming Technology*, above n50.

[52] Andrew Feenberg, *Critical Theory of Technology*, above n50; Andrew Feenberg, *Transforming Technology*, above n50; Richard Coyne, *Designing Information Technology in the Postmodern Age*, above n50.

[53] Nicholas Rescher, 'What is Value Change? A Framework for Research' in K Baier and N Rescher (eds), *Value and the Future* (The Free Press, 1969): at 48-57; see generally Peter Beilharz (ed), *Social Theory* (Allen & Unwin, 1991); Judy Wajcman, *Feminism Confronts Technology* (Allen & Unwin, 1991).

an object of control.[54] This system is characterised by an expansive dynamic which ultimately is capable of shaping the whole of social life. Heidegger argues that the technological restructuring of modern societies results in a degradation of man and being to the level of mere objects.[55]

According to Feenberg, 'the pessimism of this technological restructuring assertion is clearly apocalyptic.'[56] Regardless the basic claims are potentially believable. A situation that can serve as a humble reminder of the unintended cultural consequences of underestimating technology is the traditional family dinner. Take for example the substitution of 'fast food' for that traditional family dinner. The unity of the family, 'ritually confirmed every night, 'no longer has a comparable locus of expression. It cannot be claimed that the rise of fast food 'causes' the decline of the family but the correlation can be seen as significant.'[57]

Instrumentalists may argue that fast food supplies a nourishing meal without the need for complicated social interactions but this position is blind to the cultural implications of technology. Eating can be viewed as merely an ingestion of calories with the ritualistic aspects of food consumption being secondary to this biological need. Indeed by adopting a strictly functional approach it is possible to determine that eating (ergo healthcare delivery) is a technical operation that may be carried out with more or less efficiency. The transition 'from traditional to modernity is judged

---

[54] See Langdon Winner, *Autonomous Technology* (Oxford University Press, 1991) 6; Richard Coyne, *Designing Information Technology in the Postmodern Age*, above n50.

[55] See Andrew Feenberg, *Critical Theory of Technology*, above n50: at 7.

[56] Ibid.

[57] Don Ihde, *Philosophy of Technology*, above n10; see Andrew Feenberg, *Critical Theory of Technology*, above n50; Andrew Feenberg, *Transforming Technology*, above n50.

as progress by the standards of efficiency intrinsic to modernity but alien to tradition.'[58]

There are differences and similarities between the instrumental and substantive theories. They both share a 'take it or leave it' approach to technology. What this means is that even if you view technology as a mere instrumentality, indifferent to values, or a vehicle of cultural domination, 'in neither case can we change it.'[59] There is an overwhelming sense of technology as 'destiny' in both theories, ultimately embracing the position of technological form as beyond human intervention or repair. This is why most proposals for the reform of the regulation of technology seek only to place 'boundaries around it, not transform it.'[60]

Another perspective that has challenged the substantive and instrumental theorists is Critical Theory of technology. Critical Theory (CT) is appealing because it rejects the concept of neutrality of technology, arguing instead that 'technological rationality has become political rationality.'[61] In relation to *EPR* and e-health this view — political rationality — is supported. However it is further contended that the technological rationality can be extended to include both political and economic marketplace imperatives. Critical Theory also states that the values and interests of the elite are installed in the very design of rational procedures and machines, even before they are assigned a goal. This is an interesting argument that takes into account

[58] Andrew Feenberg, *Transforming Technology*, above n50: at 8.

[59] Langton Winner, *Autonomous Technology*, above n54; see Andrew Feenberg, *Critical Theory of Technology*, above n50: at 7.

[60] See Andrew Feenberg, *Critical Theory of Technology*, above n50; Andrew Feenberg, *Transforming Technology*, above n50.

[61] See Langton Winner, *Autonomous Technology*, above n54; Andrew Feenberg, *Critical Theory of Technology*, above n50; Richard Coyne, *Designing Technology in the Postmodern Age*, above n50.

the emergence of politics (and by association economics) as a main driver and supporter of information technology.

According to Critical Theory, the dominant form of technological rationality can be seen as neither an ideology nor neutral requirement determined by the nature of the technique. Rather it is capable of standing at the intersection between ideology and technique, where the two come together to control human beings and resources in conformity with what is called 'technical codes'. These technical codes are invisible and their invisibility sediment values, rules and procedures that routinise the pursuit of power and advantage by the dominant hegemony.[62]

The importance and relevance of these theories for the electronic healthcare regime debate is that these past insights about information technology and its appeal to neutrality, efficiency, human progress and inevitability provide fertile grounds for modern day challenges. In the 21st century a new contemporary debate about the power and desire of technology to dictate the message is emerging. The technology privacy debate includes a new breed of techno savvy scholars; and, it progresses the earlier technology theories by extending local and worldwide understanding of the threats to humanity posed by modern communication technology. What some of these later scholars argue is that information technology now poses significant threats not just too individual human rights such as individual privacy control and protection but also to democracy and democratic processes.[63]

---

[62] Andrew Feenberg, *Critical Theory of Technology*, above n50: at 14.

[63] See, eg, Tal Zarsky, "Mine Your Own Business", above n14; Evgeny Morozov, "The Real Privacy Problem", above n16; see also Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (books.google.com. 2012); Evgeny Morozov, *The Net Delusion: How Not to Liberate the World*

IV. CONTEMPORARY TECHNOLOGY PRIVACY DEBATE

There are numerous contemporary privacy theorists contributing to the ongoing debate about advancing technology and its impact upon privacy rights in the modern millennium.[64]

In 1985 Spiros Simitis, Germany's leading privacy scholar and practitioner who is also considered 'the father of modern European information privacy law,'[65] addressed the University of Pennsylvania Law School on the subject of automation of data processing technology (algorithmic regulations). His lecture on developing technology did not lose sight of the history of capitalism and democracy and saw technological changes in a far more ambiguous light.[66] In 1985 and later in 2010 he contended[67] that whatever the original incentive for computerisation may have been, processing increasingly appears as the ideal means to adapt an individual to a

(books.google.com. 2011); Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (Penguin Books, 2013); Evgeny Morozov, "Iran: Downside to the "Twitter Revolution"'(1 October 2009) 56(4) *Dissent* (00123846) 10.

[64] See, for example, Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008); Daniel Solove, Marc Rotenberg and Paul Schwartz, *Privacy, Information and Technology* (Aspen Publishers, 2006) ; Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89 *Yale Law Journal* 421; Helen Nissenbaum, *Privacy in Context* (Stanford University Press, 2010); Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011); Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009); Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press, 2006); Martha Nussbaum, *Not for Profit: Why Democracy Needs the Humanities* (Princeton University Press, 2010).

[65] See Spiros Simitis, 'Privacy Lecture' (Paper Presented at Berkeley University Law School, Berkeley California, USA, April 2010) cited in Evengy Morozov, "The Real Privacy Problem", above n16: at 39.

[66] Spiros Simitis, "The Real Privacy Problem: Technology Review" (1985) in Evgeny Morozov, "The Real Privacy Problem", above n16: at 35; Spiros Simitis, "Reviewing Privacy in an Information Society" (1987) *University of Pennsylvania Law Review*; Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" (1994) *Iowa Law Review*.

[67] Evgeny Morozov, "The Real Privacy Problem" cites Simitis, "Reviewing Privacy in the Information Society", above n16: at 35.

predetermined, standardised behaviour that aims at the highest possible degree of compliance with the model patient, consumer, employee, taxpayer and citizen.[68]

Simitis also recognised that privacy is not an end in itself. He argues instead that it is a means of achieving a certain ideal of democratic politics, where citizens are trusted to be more than just self-contented suppliers of information to all seeing, all-knowing technocrats. Three technological trends underpin Simitis's analysis. First, he warned, even back then, of 'the intensive retrieval of personal data of virtually every employee, taxpayer, patient, bank customer, welfare recipient, or car driver', which means that privacy is no longer solely a problem of some unlucky citizen caught off-guard in an awkward situation; it has become everyone's problem.[69] Second, new technologies like smart cards and videotex are making it possible to 'record and reconstruct individual activities in minute detail' but also normalise surveillance by weaving it into everyday life.[70] Third, the personal information recorded by new technologies is allowing institutions to enforce standards of behaviour, triggering 'long-term strategies of manipulation intended to mould and adjust individual conduct.'[71]

Modern institutions including governments and businesses are set to gain from this situation. For example, insurance companies can tailor cost-saving programs to the needs and demand of patients, hospitals and the pharmaceutical industry. Law

---

[68] See Evgeny Morozov, "The Real Privacy Problem", above n16: at 36.

[69] Daniel Solove, *The Future of Reputation*, above n32 [This point of excessive 'unlucky situation' surveillance opportunities is taken up by Daniel Solove in his case example, pp88-89 of the Korean 'Poop Girl' viral YouTube story]: at 1-4.

[70] See Evgeny Morozov, "The Real Privacy Problem", above n16: at 35.

[71] Ibid

enforcement can use newly available databases to identify potential criminals and locate suspects. Welfare agencies unearth fraudulent behaviour through data matching. Nevertheless according to Simitis instead of establishing greater context for decisions people would stand to lose as society becomes more automated, resulting in no one actually knowing how the algorithms work and consequently just accepting the convenient state of affairs.[72] The central problem is not necessarily the ability to personally understand the intrinsic details of technologies (like the mechanics of a car or computer algorithms) it is really about the transformational power of technology to manipulate individual desires and choices to suit its own purposes – hence 'the medium dictates the message.' Thus the balance between privacy and transparency is especially in need of adjustment in times of rapid technological change. As observed by Simitis: 'Far from being considered a constitutive element of a democratic society, privacy appears as a tolerated contradiction, the implications of which must be continuously reconsidered.'[73] It is from a democratic model of promoting and enhancing public citizen trust to be more than the recipients of technocratic 'nanny state' ideal that the thesis notion of a *Council* emerges as a significant step for ongoing healthcare privacy protection.

In 1999 Jan van Dijk, a Dutch professor of communication science, noted the rise of the networked society. He foresaw the tensions that such networked global flows of information would cause by identifying main actors designing and introducing this advanced technology 'to strengthen their own central control, be it in

[72] Evgeny Morozov, "The Real Privacy Problem", above n16: at 39

[73] Ibid; Evgeny Morozov, *The Net Delusion*, above n63.

flexible form, and limit personal autonomy and free choices at the bottom of the organisation not matching their interests.'[74]

Simitis and van Dijk's insights into the transformational power of technology to create two classes of citizens was predicted in 1963 by the German philosopher Jürgen Habermas who stated that 'an exclusively technical civilisation…is threatened…by splitting of human beings into two classes – the social engineers and the inmates of closed social institutions.'[75] In the 21st century this argument about the inevitability of technological progress and its impact of citizens is taken up by a new breed of academics and practitioners. These techno savvy scholars have a unique understanding of the complexity of technology and appreciate the broader political and economic dimension in the modern era information technology debate.[76]

We now live in a hyper-connected society that continues to be inanimate with free global flow of information where it is argued by technology advocates that 'free resources have been crucial to innovation and creativity; that without them creativity is crippled.'[77] This is especially relevant in that 'the central question becomes not whether government or the market should control a resource but whether a resource should be controlled at all.'[78] Advances in cyber-space and internet technology have

---

[74] Jan van Dijk, *The Network Society* (Sage Publications, 2012); Jan van Dijk, *The Deepening Divide: Inequality in the Information Society* (books.google.com. 2005); Jan van Dijk and Kenneth Hacker, 'The Digital Divide as a Complex and Dynamic Phenomenon' (2003) in Jan van Dijk, *The Information Society* (Taylor & Francis, 2003); Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Penguin Books, 2012), cites Jan van Dijk, *The Network Society,* above n63*:* at 220.

[75] Jurgen Habermas quoted in Evgeny Morovoz, *The Net Delusion*, above n63: at 37.

[76] See Tal Zarsky, "Mine Your Own Business", above n14; Jaron Lanier, *You Are Not A Gadget*, above n14; see generally Clay Shirky, Tim Wu, Sacha Lobo and Ethan Zuckerman.

[77] Evgeny Morozov, "The Real Privacy Problem", above n16: at 37.

[78] Ibid.

resulted in a proliferation of social networking sites such as YouTube, Twitter, Facebook and Instagram. As previously noted, social networking transforms how people communicate and socialise with each other. These sites provide great entertainment opportunities and many benefits but there can be numerous downsides to these benefits, including the seduction of a new generation of people to voluntarily release their 'sensitive' personal information which ultimately diminishes their ongoing rights to privacy.[79]

Our culture is shedding traditional experts and creating new ones[80] and overwhelming those institutions that have provided mechanisms of information control such as families, health services, education institutions and law courts with increasing information requirements.[81] According to Zarsky and Mayer-Schonberger, technology has moved beyond mere recording and surveillance of personal information to include the development of sophisticated programs that allow analysis of this data.[82] Recording is easy and in the world of high technology where memory

---

[79] See Fitzgerald, et al, *Internet and E-Commerce Law*, above n18 [Fitzgerald identifies that in order to participate in social network sites, it is often necessary to provide 'voluntary' detailed personal information to the network]: at 39.

[80] See, for example, technology experts, designers of technology, etc.

[81] See, for example, Neil Postman, *Technopoly*, above n4. 'The rule of law is an oversimplification' and Postman argues that therein lays the power of theories, 'to oversimplify and assist believers in organising, weighting and excluding information': at 77 also noting that 'The weakness is that it is an oversimplification that is vulnerable by attack by new information' and arguing that 'When there is too much information to sustain any theory, information becomes essentially meaningless': at 77.

[82] See Tal Zarsky,"Mine Your Own Business", above n14: at 1; Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age,* above n63; see generally European Union Commission, '*Right to be Forgotten Ruling*' (c-131/12) [this ruling resulted from a citizen complaint]. In 2010 a Spanish citizen lodged a complaint against a Spanish newspaper with the National Data Protection Agency & against Google Spain and Google Inc. He requested that the newspaper is required either to remove or alter personal data relating to him. In its ruling of 13 May 2014 the EU Court held 'that there is a 'right to be forgotten' – individuals have a right – under certain conditions – to ask search engine to remove links with personal information about them (this applies if information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing' (Para 93 of the ruling). It held that 'a case by case assessment is needed to consider the type of information in question' (balanced against freedom of

is cheap and nothing is forgotten or lost in oblivion, governments and corporations invest in storage of trivial information hoping to reap the benefits in the future.

It is possible to analyse databases using simple statistical 'query' and that specific information can be retrieved using various types of information about the database as a whole. Advanced practices include segmenting the database into groups and analysing each sub-database on its own or as a comparative analysis. The limitation with this type of query is that unless one knows what questions to ask present applications may be inadequate for prediction or marketing purposes.[83]

In the competitive environment, tools that allow governments and organisations to reveal deeper and unknown connections about individuals, families and society are now required. In light of advancing sophisticated mega data-analysis and data-mining possibilities conducted by both government and industry the issue of individual privacy protection rights to exercise any 'control' over personal information is further diminished and takes on a new urgency, particularly in relation to the collection and 'sharing' of *EPR* and e-health records.[84] According to Zarsky, the latest advances in information research technology such as data-analysis and data-mining include not just an ability to collect and access personal information but the capacity to generate detailed profiles about a person. This form of analysis is available through hi-tech data-mining opportunities.

---

expression and the media). European Commission, 1995 Data Protective Directive, Article 12 and Article 17 [includes 'the right to be forgotten and to erase' and the 'right to erase'].

[83] Tal Zarsky, "Mine Your Own Business", above n14.

[84] See the College of Australian Healthcare Informatics and the Asia Pacific Healthcare Informatics Agreement to share healthcare information between China, New Zealand and Australia (signed in 1994).

Ann Cavoukian, Canadian Privacy Commissioner, as well as other privacy scholars[85] believe that the only way that adequate privacy and security protection mechanisms will form part of system design is if the time is taken to firmly embed privacy and security protection as part of the system in the first instance.[86] Morozov warns that if adequate privacy and security mechanisms are not included there is a very real risk of not being able to fix this problem later. As recognised by NEHTA, embedding adequate privacy and security protection mechanisms in *EPR* and e-health will take time, require resources and is contingent on learning from other countries experiences in this area.

V. NEW CHALLENGES FOR ELECTRONIC HEALTHCARE SYSTEMS AND PRIVACY PROTECTION RIGHTS

It can be observed that the growing effects of computer and information revolution now surpass any previously held notions of technologies potential impact on individual identity and cultural practices. As a result of rapidly developing technology over the past decade, new challenges have arisen that were not envisaged by the Australian Government's original e-health and privacy protection strategies.[87]

---

[85] See Evgeny Morozov, "The Real Privacy Problem", above n16.

[86] See Ann Cavoukian, *Privacy by Design: Strong Privacy Protection – Now, and Well into the Future* (2011) (A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners, 2011). The Report argues that privacy and security default must be embedded into technology; see also Ann Cavoukian, Angus Fisher, Scott Killen and David Hoffman, "Remote Home Health Care Technologies: How to Ensure Privacy? Build it in: Privacy by Design" (22 May 2010) *Springerlink.com* (online).

[87] See, for example, Australian Government, COAG, *Healthcare Identifiers and Privacy: Discussion Paper on Proposals for Legislative Support* (July 2009); Australian Government, *PCEHR System: Legislation Issues Paper* (April 2011); NEHTA, *Concepts of Operations,* above n3.

These challenges include the development of highly intrusive and extremely sophisticated technical improvements such as data-linkage capabilities, data-mining, informatics, biometrics and surveillance opportunities. The considerable bearing of these advanced technologies on everyday human interaction clearly indicate that government has gravely underestimated the degree of privacy protection intervention necessary in the new digital economy. Consequently existing legal and governance *EPR* and e-health privacy measures are seriously compromised and do not go far enough to provide long-term solutions to emerging modern day technology privacy and security risks.[88]

Indeed the thesis contends that privacy protection is no longer just about protecting an individual's privacy rights in the new information economy. The contemporary debate reflects the growing influence and extending reach of modern communication technology, capturing its enduring ability to construct social reality by seducing and dominating citizens, by insisting upon total unquestioning dedication to its continuing progress and determining our identity by simultaneously shaping desires to fit our new digital identities. The emerging privacy technology debate demands consideration of the broader political and economic agenda, including identifying the ideology that underpins and drives modern technology.

VI. CONCLUSION

It is within this wider contemporary framework that technology privacy as a dynamic work in progress and not just a static process or legal solution must be conceived.

[88] See chapter 6, pp186-234 on *PCEHR* and e-health governance; chapter 7, pp238-261 for details and further discussion of the *Council*.

Consequently there is an urgent need to reconceptualise both technology and privacy and reinforce current understanding of technology privacy to include the introduction of a *Council*. This would represent a preliminary but significant first positive step towards localising and recapturing not only our individual identity which relies on privacy as a human right but also broader democratic rights currently under threat by expanding information economy and intrusive and demanding 'tools' utilised by technology.

In summary, this chapter in combination with other thesis chapters provides significant historical and theoretical background information about technology development and healthcare privacy protection issues. Chapter 4 extends this contextual understanding of the impact of healthcare privacy protection rights by exploring the theoretical development of the concept of privacy and its ongoing relevance to healthcare in Australia.

CHAPTER 4

UNDERSTANDING PRIVACY

This chapter argues that in the modern information era there is an urgent need to reconceptualise privacy and privacy rights. Further, it is contended that the new electronic healthcare regime challenges long standing expectations of individual healthcare privacy protection by adopting digital information *sharing* and that this is problematic for both healthcare providers and consumers in relation to long-established professional privacy expectations and obligations and that this impacts on individual privacy rights.

I. EVOLVING CONCEPTUAL THEORIES IN PRIVACY

Privacy discourse in Australia and internationally is widely premised upon Western liberal democratic ideology with an emphasis on advancing international economic imperatives.[1] Over the last few decades, privacy, its relationship with technology and

[1] See David Lindsay, "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law" [2005] *Monash University Law Review* 4; see also Simon Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001); see Fredrick Abbott, 'Emerging Market Pharmaceutical Supply: A Prescription for Sharing the Benefits of Global Information Flow' in Ramesh Subramania and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011); Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press, 2006): at 91. It can also be noted, that given the prominence of Western Liberation, the largest body of privacy materials emanates from North America; although this trend is being challenged by a new breed of contemporary international and European savvy techno theorists (for example, Tal Zarsky and Viktor Mayer-Schonberger); see also Evgeny Morozov, "The Real Privacy Problem" (22 October 2013) 116(6) *MIT Technology Review* 32-43.

its impact on society has occupied the minds of eminent scholars, particularly in relation to the continuing convergence of computer and communication technology in the modern information economy.[2] Similar to Australia, international privacy scholarship is robust and there is vast literature that attempts to address the question 'what is privacy?'[3]

Legal and privacy scholars, philosophers and practitioners persist in their search for a fundamental, distinctive and internally consistent core to defining privacy. However, privacy is considered a multifarious concept that influences manifold areas of physical and psychological existence and the social environment. Accordingly, legal privacy theorist, Daniel Solove observes that finding an all-encompassing definition can be likened to finding the 'holy grail.'[4] Regardless of these barriers, he notes that the search for privacy's essence, character and the meaning should not be abandoned because privacy analysis supports continuing understandings of its importance and relevance in a constantly changing world.[5]

II. MORAL THEORIES

[2] See Daniel Solove, *The Digital Person* (New York University Press, 2004); see also Kathy Bowrey, *Law and Internet Culture* (Cambridge University Press, 2005); Daniel Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Stanford University Press, 2011).

[3] See, eg, Meredith Carter, "Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers" (2002) 172 *Medical Journal of Australia*; Lyria Bennett-Moses, "Recurring Dilemmas: The Law's Race to Keep up with Technology Changes" [2007] *University of New South Wales Law Review Series* 21; Adam McBeth, "Privatising Human Rights: What Happens to State's Human Rights Duties When Services are Privatised?" (2004) 5(1) *Melbourne Journal of International Law* 133; Megan Richardson, "Wither Breach of Confidence: A Right of Privacy for Australians" [2002] *Melbourne University Law Review* 20.

[4] Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008) 12-13.

[5] See Daniel Solove, *The Digital Person*, above n2.

Normative moral theories such as Consequentialists and Non-consequentialists theories continue to occupy a prominent role in Australian and international privacy debate, as does the private-public dichotomy view of privacy.[6] Historically the public-private dichotomy remains a popular division in privacy analysis discourse.[7] This convenient conceptual division distinguishes between public and private existence by determining whether any definable spheres exist and if the boundaries of the private sphere are traditionally defined by public agents.[8] The term public and private are used to provide structure to the activities of lives and the law. The liberal concept of the private typically refers to behaviour and activities not regulated by law. In contrast, the public sphere consists of the world of politics and state activities.[9]

---

[6] See Brett Mason, *Privacy without Principle* (Australian Scholarly Publishing, 2006). Mason states that 'the public/private divide has operated, and continues to operate, as an 'ideological tool' and that 'liberal democracies demonstrate a preoccupation with the public/private dichotomy': at 10-21; see also David Lindsay, "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", above n1; Australian Law Reform Commission (ALRC), *Review of Australian Privacy Law*: Discussion Paper 72 (September 2007). In *Discussion Paper 72*, the ALRC reviewed international and Australian privacy conceptual scholarship and law in the area: at 114-124; see Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (The Federation Press, 2005). Doyle and Bagaric observe that normative moral theories have proliferated over the last two or three decades; Doyle and Bagaric discusses the development of consequentialist moral theories and non-consequentialist (or deontological) theories such as human rights: at 20-24; see Danuta Mendelson, "Electronic Medical Records: Perils of Outsourcing and the *Privacy Act* 1988 (Cth)" (2004) 12 *Journal of Law and Medicine* 8; see also Bernadette McSherry, "Ethical Issues in Health*Connect's* Shared Electronic Health Record System" (2004) 12 *Journal of Law and Medicine* 60; Graham Greenleaf, Nigel Waters and Lee Bygrave, "Implementing Privacy Principles: After 20 Years, It's Time to Enforce the *Privacy Act*" [2007] *University of New South Wales Law Review Series* 31; Margaret Otlowski and Robert Williamson, "Ethical and Legal Issues and the "New Genetics"" (2003) 178 *Medical Journal of Australia* 582; Donald Lindberg and Betsy Humphreys, "Medicine and Health on the Internet" (1998) 280 *Medical Journal of Australia* 1303.

[7] Doyle and Bagaric, *Privacy Law in Australia*, above n6; see Brett Mason, *Privacy without Principle*, above n6; see also S Benn and G Gaus (eds), *Public and Private in Social Life* (St Martin's Press, 1983); Hannah Arendt, *The Human Condition* (University of Chicago Press, 1958); see Jurgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (The MIT Press, 1989); Amitai Etzioni, *The Spirit of Community* (Touchstone Books, 1994).

[8] Brett Mason, *Privacy without Principle,* above n6: at 10-11.

[9] Ibid; see also Graeme Laurie, *Genetic Privacy* (Cambridge University Press, 2002) 28.

Although extensive scholarly and judicial writing on privacy has produced many different conceptions of privacy, it is generally agreed by theorists that within privacy discourse there are a number of common denominators that transcend national and international boundaries. These denominators provide a basis upon which privacy as a utility, value or right can be further conceptualised. Common denominators include 'the right to be let alone', 'limited access to self', 'secrecy', 'personhood', 'control-over-personal-information' and 'intimacy and isolation'.[10] These conceptions often overlap, but each has a distinctive perspective on capturing the essence of privacy, particularly from an individual privacy rights approach.

A. *The right to be let alone*

The 'right to be let alone' is Warren and Brandeis's famous formulation in their article "The Right to Privacy."[11] Its significance to the privacy debate is that it provides the basis for further privacy analysis and is often referred to as the most 'influential law review article of all.'[12] Warren and Brandeis began the article by describing new technological developments that were posing a potential threat to privacy such as the

[10] See Daniel Solove, *Understanding Privacy*, above n4: at 12-13; see also Daniel Solove, *The Future of Reputation* (Yale University Press, 2007); Daniel Solove, *Nothing to Hide*, above n2.

[11] Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

[12] See Richard Turkington, "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Privacy" (1990) 10 *Northern Illinois University Law Review* 479; see also Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89 *Yale Law Journal* 421; Charles Fried, "Privacy" (1968) 77 *Yale Law Journal* 475; Tom Gerety, "Redefining Privacy" (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 233; Irwin Kramer, "The Birth of Privacy Law: A Century Since Warren and Brandeis" (1990) 39 *Catholic University Law Review* 703; D McCormick, "Privacy: A Problem of Definition" (1974) 1 *British Journal of Law and Society* 75; W A Parent, "New Definition for Privacy for the Law" (1983) 2 *Law and Philosophy* 305; W Prosser, "Privacy: A Legal Analysis" (1960) 48 *California Law Review* 338.

newspaper press and instantaneous photographs. They were also concerned not only with the new technology but at the time with how it would intersect with the media.[13]

According to Warren and Brandeis, 'the-right-to-be-let-alone' further highlights a general right of the 'immunity of the person to one's personality'.[14] The authors' point out various limitations of established legal actions such as defamation law as about protecting 'reputation' and explain that privacy as involving 'injury to feelings' can also be captured by the law. The impact of the article on U.S. jurisprudence cannot be questioned because it brought significant attention to privacy, resulting in a number of common law tort actions to protect privacy.[15] The article also framed further scholarly and practitioner discussion of privacy in the U.S. throughout the 20th century.[16]

B. *Limited access to self*

A subset of 'right to be let alone' is 'limited access to self'. The conceptual view of privacy as relying on 'limited access to the self' emphasised the individual's desire for concealment and for being apart from others. In the late 19th century, Godkin advanced an early version of the limited access theory, observing that 'nothing is

---

[13] Warren and Brandeis, "The Right to Privacy", above n11: at 196.

[14] Warren and Brandeis, "The Right to Privacy", above n11.

[15] See Ruth Gavison, "Too Early for a Requiem: Warren and Brandeis were Right on Privacy v Free Speech" (1992) 43 *South Carolina Law Review* 437: at 438; see also Ruth Gavison, "Privacy and the Limits of the Law", above n12: at 441; Harry Kalven, "Privacy in Tort Law: Were Warren and Brandeis Wrong?" (1966) 31 *Law and Contemporary Problems* 326; Benjamin Bateman, "Brandeis and Warren's "The Right to Privacy" and the Birth of the Right to Privacy" (2002) 69 *Tennessee Law Review* 623.

[16] *Olmstead v United States* 277 U.S. 438, 466 (1928) [in Olmstead, the Court held that wiretapping was not a violation under the Fourth Amendment of the U.S. Constitution 'because it was not a physical trespass into the home']: at 442; see also *Katz v United States* 389 U.S. 347 (1967). In its Fourth Amendment jurisprudence, as well as its protection of the right to privacy, the Supreme Court invoked Brandeis's formulation of privacy, as "the right to be let alone": at 350; Elbridge Adams, "The Right of Privacy, and its Relation to the Law of Libel" (1905) 39 *American Law Review* 37.

better worthy of legal protection than private life, in other words, the right of every man to keep his affairs to himself.'[17]

Despite similarities 'limited access to self' is not equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of 'limited access' as well as the 'right-to-be-let-alone' conception. These theories extend more broadly than solitude, embracing freedom from government interference, including intrusions by the media and others. 'Limited access' conceptions recognise that privacy extends beyond merely being apart from others.[18]

Contemporary privacy theorist, Sissela Bok, has advanced a more sophisticated version of 'limited access' conception; he considers that privacy is 'the conditions of being protected from unwanted access by others – of physical access, personal information, or attention.'[19] According to Ernest Van Den Haag, 'Privacy is the exclusive access of a person (or other legal entity) to a realm of his own.'[20] Consequently the right to privacy entitles one to exclude others from watching, utilizing, or invading his private realm.[21] Legal theorist, Anita Allen asserts that 'a

---

[17] E L Godkin, "The Rights of the Citizen - To His Own Reputation" (July-December 1890) *Scribner's Magazine*, 65; E L Godkin, "Libel and its Legal Remedies" (1880) 12 *Journal of Social Science* 69.

[18] See Daniel Solove, *Understanding Privacy*, above n4: at 19; Daniel Solove, *Nothing to Hide,* above n2.

[19] Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Random House, 1983) 10-11; Hyman Gross, "The Concept of Privacy" (1967) 43 *New York University Law Review* 34; see also Braxton Graven, "Personhood: The Right to be Let Alone" (1976) *Duke Law Journal* 699.

[20] Van Den Haag, 'On Privacy' in Roland Pennock and J Chapman (eds), *Nomos XIII: Privacy* (Roland Pennock & J Chapman, 1971): at 149.

[21] Ibid.

degree of inaccessibility is an important necessary condition for the apt application of privacy.'[22]

In common with other critics of this theory, the thesis rejects 'limited access' to the self as too limited. It is an inadequate privacy definition because without a notion of what matters are private, limited access conceptions do not identify the substantive matters for which access would implicate privacy. In addition the theory provides no understanding as to the question of degree of access necessary to constitute privacy violations thus limiting its value as an all-encompassing privacy definition.[23]

C. *Secrecy*

One of the most common understandings of privacy is that it constitutes the 'secrecy' of certain matters.[24] 'Secrecy' of personal information is a way to 'limit access to self'.[25] Under this view privacy is violated by public discourse of previously concealed information.[26] Richard Posner, a law and economics scholar is critical of this

---

[22] Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Allen Rowman & Littlefields Publication, 1988) 10. For additional information and argument on limited-access conceptions; see Edward Shils, "Privacy: Its Constitution and Vicissitudes" (1966) 31 *Law and Contemporary Problems* 281 [where privacy 'is constituted by the absence of interaction or communication or perception within contexts in which such interaction, communication, or perception is practicable']: at 281.

[23] Anita Allen, *Uneasy Access*, above n22: at 7; see Sidney Jourard, "Some Psychological Aspects of Privacy" (1966) 31 *Law and Contemporary Problems* 307; Ruth Gavison, "Privacy and the Limits of the Law", above n12; see also Daniel Solove, *The Digital Person*, above n2: at 20-21; Daniel Solove, *Understanding Privacy*, above n4.

[24] See Edward Richard Parker, "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 [where Parker seeks to articulate some characteristics common to all or identify some of different personal interests]; Ruth Gavison, "Privacy and the Limits of the Law", above n12; Warren and Brandeis, "The Right to Privacy", above n11.

[25] See Edward Bloustein, "Privacy as an Aspect of Human Dignity" 39 *New York University Law Review* 962 [where Bloustein proposes a general theory of individual privacy, which will reconcile the divergent strands of legal development]; Edward Richard Parker, "A Definition of Privacy", above n24; see also Thomas Scanlon, "Thomson on Privacy" 4 *Philosophy and Public Affairs* 315.

[26] See Charles Fried, "Privacy", above n12 [in *Privacy* Fried defines privacy as 'control over knowledge about oneself' that is necessary to 'protect fundamental relations of respect, love, friendship and trust based upon values of autonomy']: at 477, 483; see also Tom Gerety, "Redefining Privacy", above n12;

conception, seeing privacy protection as a form of 'interested economic behaviour, aimed at concealing true but harmful facts about oneself for one's own gain.'[27] Posner asserts that people 'want to manipulate the world around them by selective disclosure of facts about themselves.'[28] Sidney Jourard supports Posner's concept of privacy; according to him it is 'an outcome of a person's wish to withhold from others certain knowledge as to his past and present experience.'[29] Posner and Jourard's 'secrecy' view of privacy suggests that having 'secrets' is somehow deceptive because it is about hiding something that may define the person.

The conception of privacy as concealing information about the 'self' continues to underpin the U.S. constitutional right to information privacy cases such as *Griswold v Connecticut*[30] and *Roe v Wade*.[31] Critics of the theory have claimed that understanding privacy as 'secrecy' conceptualises privacy too narrowly.[32] For instance, Edward Bloustein contends that this conception of privacy fails to recognise group privacy.[33] Judith DeCrew is also critical of 'secrecy' arguing that the harm caused by an invasion of privacy and understanding privacy violation involves more than avoiding

---

W A Parent, "New Definition for Privacy for the Law", above n12; W A Parent, "Recent Work on the Concept of Privacy" (1993) 20 *American Philosophical Quarterly* 341.

[27] Richard Posner, *Economics of Justice* (Harvard University Press, 1981) 272-273; see also Richard Posner, *Economic Analysis of Justice* (Harvard University Press, 1998) [Posner's conception of privacy is infused with his own normative assessment of privacy as a form of deception]. According to Posner, the 'economist sees a parallel to the efforts of sellers to conceal defects in their products': at 46.

[28] Richard Posner, *Economics of Justice*, above n27: at 273.

[29] Sidney Jourard, "Some Psychological Aspects of Privacy" (1966) 31 *Law and Contemporary Problems* 307: at 307.

[30] *Griswold v Connecticut* (1965) 381 U.S. 479.

[31] *Roe v Wade* (1973) 410 U.S. 113.

[32] See Edward Shils, "Privacy: Its Constitution and Vicissitudes" (1966) 31 *Law and Contemporary Problems* 281: at 305.

[33] Edward Bloustein, "Privacy as an Aspect of Human Dignity", above n25: at 123.

disclosure. She argues that it involves the individual's ability to ensure that personal information is used for the purposes he or she desires.[34]

The 'secrecy' view is rejected by the thesis because it provides a very limited view of privacy. It mainly conceives privacy as a narrow individualistic self-serving interest that operates within an economic context. This limited perception suggests that people who have secrets have something to hide. Rather than recognising 'secrecy' as a positive human option, which can give people the necessary freedom to limit the effects of embarrassing information and awkward moments that make no difference to who or what they are now, this narrow focus defines secrecy as a negative trait in all circumstances.

A common retort to 'secrecy' as a viable option is the 'nothing to hide' argument.[35] The 'nothing to hide' debate relates to the false trade-off between privacy and security in the digital era.[36] Advocates of this notion contend that privacy must be sacrificed for security. Pro-security proponents argue that if you have 'nothing to hide' you should not worry about laws that favour promoting government surveillance security at the expense of individual privacy protection rights.[37] If you have 'nothing to hide' you have nothing to fear about surveillance, and security and decreasing privacy rights. Solove argues that the ensuing debate between privacy and

---

[34] See Judith Wagner DeCrew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997) 48; Judith Jarvis Thomson, 'The Right to Privacy' in Ferdinand D Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (books.google.com. 1984): at 272.

[35] Daniel Solove, *Nothing to Hide,* above n10.

[36] Ibid.

[37] Daniel Solove, *Nothing to Hide,* above n10 [Solove questions what we understand by the term 'national security' and observes that 'national security' has often been abused as a justification not only for surveillance but also for maintaining the secrecy of government records as well as violating the civil liberties of citizens]: at 66.

security has been framed incorrectly as a 'zero-sum game' in which people are forced to choose between one value and the other.[38] He observes that protecting privacy is not fatal to security measures; it merely involves adequate oversight and regulations.[39]

D. *Control-over-personal-information*

A popular theory of privacy is that it enables a person 'control-over-personal-information'[40] it can be viewed as a sub-set of the 'limited access' conception. This particular denominator is appealing as a way of protecting privacy in the area of digital information such as found in new *EPR* and e-health systems.[41] The theory focus is on information; however it excludes those aspects of privacy that are not informational such as the right to make some fundamental decisions about one's body or reproduction. According to Alan Westin, 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.'[42] Therefore 'privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.'[43]

Critics of the theory have argued that the 'control-over-information' conception focuses on all information over which individuals want to retain control, but privacy is not simply a subjective matter of individual prerogative, it is also an issue of what

[38] Daniel Solove, *Nothing to Hide*, above n10.

[39] Ibid 1.

[40] See Alan Westin, *Privacy and Freedom* (Bodley Head, 1967).

[41] See ALRC, Discussion Paper No 72, above n6: at 112.

[42] Alan Westin, *Privacy and Freedom*, above n40, 7; ALRC, Discussion Paper No 72, above n6; Charles Fried, "Privacy", above n12: at 482.

[43] Charles Fried, "Privacy", above n12: at 483

society deems appropriate to protect.[44] Some theorists attempt to define the scope of what constitutes personal information over which individuals have control. For instance, Richard Parker defines the scope of personal information extremely broadly: 'Control over who sees us, hears us, smells us, and tastes us, in sum, control over who can sense us, is the core to privacy.'[45] This definition is limited because it would preclude most interpersonal contact in society as constituting a privacy invasion. We are frequently seen and heard by others in circumstances that would not suggest even the slightest invasion of privacy. Other scholars limit the scope of personal information to that which relates to the individual.[46]

In addition to falling short of adequately defining the scope of information, 'control-over-information' conception fails to define what is meant by control. Theorists provide very little insight on what control really entails and it is often conceived as too broad or too narrow. Frequently control is understood as a form of 'ownership' of information. For instance Westin concludes that 'personal information should be defined as a property right.'[47] This notion is partly embodied in tort law

---

[44] Ferdinand Schoeman, 'Privacy: Philosophical Dimensions of the Literature' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology*, above n34. Schoeman, for example, observes that 'regarding privacy as a claim or entitlement to determine what information about oneself is available to others … [wrongly] presumes privacy is something to be protected at the discretion of the individual to whom the information relates': at 3; see Alan Westin, *Privacy and Freedom*, above n40.

[45] See Richard Parker, "A Definition of Privacy", above n24: at 280

[46] See, for example, Richard Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 *Georgetown Law Journal* 2381 {Murphy defines the scope of personal information as consisting of 'any data about an individual that is identifiable to that individual': at 2383. Murphy's definition is far too broad because there is a significant amount of information identifiable to us that we do not deem as private', thus this theory provides no reasonable limitation in scope]: at 2382

[47] See Alan Westin, *Privacy and Freedom*, above n40.

such as doctrines of appropriation and passing off, which protects people against other's using their image or likeness for commercial gain.[48]

Extending property rights to personal information has difficulties because information can be easily transmitted and once known by others cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously within the minds of millions. This accounts for why intellectual-property law protects particular tangible expressions of ideas rather than the underlying ideas themselves.[49] Further there is a problem of viewing personal information as equivalent to any other commodity this is because it is often formed in relationships with others. All parties to that relationship have some claim to the information. For instance, *EPR* information is the result of the interaction between the healthcare provider and patient and it may also contain detailed personal information about the patient's family.[50]

Theorists such as Paul Schwartz and Charles Fried[51] consider the 'control-over-information' conception as being too narrow because it focuses too heavily on individual choice. The assumption that individuals have autonomy to exercise control over their personal information in all situations fails to realise 'that individual self-determination is itself shaped by the processing of personal data.'[52] Schwartz argues

---

[48] See Bruce Clarke, Brendan Sweeney and Mark Bender, *Marketing and the Law* (LexisNexis, 2011) 175.

[49] Clarke, Sweeney and Bender, *Marketing and the Law*, above n48; see also Daniel Solove, *Understanding Privacy,* above n4: at 27.

[50] See Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, 2002) [Laurie examines the question of genetic information and the 'right to know' from the perspective of individuals, family and employees].

[51] Charles Fried, "Privacy", above n12: at 475.

[52] See Paul Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 *Vanderbilt Law Review* 1609: at 1661.

that the assumption that individuals are able to exercise meaningful choice with regards to their information must be questioned, given the disparities in knowledge and power in bargaining over the transfer of their information is limited.[53] The implication is that privacy involves not only individual control, but also the social regulation of information. In other words, privacy is an aspect of social structure, architecture of information regulation and not just a matter for the exercise of individual control.

The thesis agrees with the proposition that conceptualising privacy as 'control-over-information' is limited because it is too vague, too broad and often too narrow. It is too vague or broad because it fails to define what 'control' entails. It is too narrow because it reduces privacy to just informational concerns, omits decisional freedom from the realm of privacy and focuses too much on autonomy and individual choice. As a result of these shortcomings the thesis proclaims that healthcare privacy protection involves more than just putting in place pragmatic information privacy legislation and regulations, it necessitates not only recognition of privacy but also combining such recognition with statutory regulations and governance-extending privacy-protection mechanisms such as the proposed addition of a *Council* as part of the governance long term solution.[54]

E. *Personhood*

Another prevalent privacy theory is that it refers to 'personhood'. This theory, unlike other privacy theories is constructed around the protection of the integrity of

[53] Pauls Schwartz, *Privacy and Democracy in Cyberspace*, above n52.

[54] See chapter 6, pp186-234 for discussion on *PCEHR* and e-health governance.

personality and thus protects individuality and dignity. This theory builds upon Warren and Brandeis's notion of 'inviolate personality'.[55] The theory of privacy as personhood differs from other theories because it is constructed around a normative end of privacy, that is, the protection of the integrity of personality. It is a popular theory because it appeals to privacy concerns beyond mere physical protections. It acknowledges both the physical and psychological dimensions of privacy rights.

According to Edward Bloustein, the concept of personhood privacy protects the individual against conduct that is 'demeaning to individuality' or 'an affront to personal dignity'.[56] Philosopher Jeffrey Reiman also recognises a personhood component of privacy.[57] Stanley Benn developed a concept of 'personhood' privacy, which is based on 'respect for someone as a person, as a chooser, implies respect for him as one engaged in a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited intrusion as watching.'[58] This 'personhood' concept of privacy is appealing in the current privacy debate because of the growth of surveillance technology in society.[59]

Jeffrey Rosen's notion of the 'unwanted gaze,' which examines the legal, technological and cultural changes that have undermined the ability to control how much information about ourselves, is communicated to others represents the notion

---

[55] See Samuel Warren and Louis Brandeis, "The Right to Privacy", above n11.

[56] Edward Bloustein, "Privacy as an Aspect of Human Dignity", above n25.

[57] Jeffrey Reiman, 'Privacy, Intimacy, and Personhood' in Ferdinand Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, above n44: at 314.

[58] See Stanley Benn, 'Privacy, Freedom, and Respect for Persons' in Pennock and Chapman (eds), *Nomas XIII: Privacy*, above n20: at 149.

[59] See Daniel Solove, *Understanding Privacy*, above n4.

of being 'watched.'[60] Rosen's view of being constantly watched and the effects this has on individuals (and personhood) provides a useful critique of fear factors such as terrorism, globalisation, information economy and advancing surveillance technology concerns.[61] Respect for someone as a person, as a chooser, implies respect for that person as one engaged in a kind of self-creative enterprise, which can be disrupted, distorted or frustrated by an intrusion such as watching. As Benn explains that 'being an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes.'[62] He contends that surveillance restricts an individual's range of choices and thus limits freedom.[63] Accordingly, privacy is about respect for personhood, with personhood defined in terms of the individual's capacity to choose.[64]

However theories of personhood fail to elucidate what privacy is because they often do not articulate an adequate definition of personhood. Freund's notion of attributes irreducible in one's selfhood is far too vague and merely substitutes 'selfhood' for 'personhood.'[65] Bloustein's examination of personhood as 'individuality' fails to define the scope or nature of individuality.[66] Personhood

---

[60] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, 2000) 4.

[61] Jeffrey Rosen, *The Unwanted Gaze*, above n60; see also Jeffrey Rosen, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror" (2004) 46 *Arizona Law Review* 607.

[62] Stanley Benn, 'Privacy, Freedom, and Respect for Persons' in Pennock and Chapman, *Nomas XIII: Privacy*, above n20: at 150.

[63] Ibid.

[64] Daniel Solove, *Nothing to Hide*, above n10: at 29.

[65] Paul Freund, 'Address to the American Law Institute' (Address to the 52nd Annual American Law Institute Meeting, 1975): at 42; see also Braxton Graven, "Personhood: The Right to be Let Alone", above n19 cites Freund's formulation of personhood in the 'Address to the American Law Institute': at 702.

[66] Edward Bloustein, "Privacy as an Aspect of Human Dignity", above n25: at 971.

theories, while appealing, are consequently too broad or too vague. Personhood is often defined as a type of autonomy.[67]

Jed Rubenfeld offers an alternative conception that defines the right to privacy through a sophisticated account of the problems of 'personhood' theory of privacy in his article — *The Right to Privacy*.[68] He identifies his personhood thesis as: 'where our identity or self-determination is at stake, there the state may not interfere.' He offers an alternative conception that defines the right to privacy as conduct that personhood purports to protect as 'essential to the individual's identity.' Unfortunately it 'inadvertently reintroduces into the privacy analysis the very premise of the invidious uses of state power it seeks to overcome.' Thus when the state endeavours to protect personhood, it must adopt and enforce its own conception of individual identity, impinging upon the freedom of individuals to define for themselves what is central to their identities.[69]

F. *Intimacy and Isolation*

The final common denominator understands privacy as a form of *intimacy and isolation*. This theory, which is closer to the one embraced for the purpose of this thesis, appropriately recognises that privacy is essential not just to self-creation but also for

---

[67] Edward Bloustein, *Privacy as an Aspect of Human Dignity*, above n25.

[68] Jed Rubenfeld, "The Right to Privacy" (1989) 102 *Harvard Law Review* 801 [Rubenfeld identifies the 'creeping totalitarianism, an unarmed occupation of individual's lives' of the 'progressively more normalising state as a major consideration for understanding privacy']: at 802. Privacy is invoked 'only where the government threatens to take over or occupy our lives – to exert its power in some way over the totality of our lives.' This conception of privacy as a right against totalitarianism appeals to the ongoing privacy debate in Australia, especially in light of the federal Coalition Liberal Government's privatisation policy and actions relating to the downgrading of freedom of information services and rationalisation of Australian Information Commission; see federal *Budget* 2013-2014.

[69] Jed Rubenfeld, "The Right to Privacy", above n68; see also Daniel Solove, *Nothing to Hide*, above n10: at 32.

human relationships. In *Privacy, Intimacy and Isolation*, Julie Innes advances an intimacy conception of privacy 'the content of privacy cannot be captured if we focus exclusively on information, access, or intimate decisions because privacy involves all three areas.'[70] In contrast with many proponents of privacy as intimacy, Innes recognised the need to define 'intimacy'. According to Innes 'intimacy stems from something prior to behaviour' it is an individual's motives that matter.[71] However, she notes the difficulty of adequately defining intimacy and this limits the value of this theory as an all-encompassing definition of privacy.[72]

Privacy theorist Charles Fried also advances 'intimacy' as a concept that locates the value of privacy and circumscribes the scope of information over which we should have control.[73] He positions 'intimacy' as 'sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone.'[74] He contends that by conferring this right 'privacy creates the moral capital which we spend in friendship and love.'[75] Along similar lines, James Rachels asserts that privacy is valuable because 'there is a close connection between our ability to control who has access to us and the information about us, and our ability to create and maintain different sorts of social relationships with different people.'[76] For theorists such as Fried and Rachels – intimate information is that which

---

[70] Julie Innes, *Privacy, Intimacy, and Isolation* (Oxford University Press, 1992) 56.

[71] Ibid.

[72] Ibid 76, 77.

[73] Charles Fried, "Privacy", above n12.

[74] Ibid.

[75] Ibid.

[76] James Rachel, 'Why is Privacy Important?' in Ferdinand Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, above n34: at 292.

individuals want to reveal only to a few people. Because healthcare information may include 'sensitive' and 'intimate' information, the e-health concept of 'sharing' health information with an ever expanding group of healthcare providers and yet unidentified third parties is likely to preclude, despite *consumer-control* focus, individual choice about what information is collected and with whom it is ultimately shared.[77]

Given the above analysis of privacy denominators and in combination with other scholarly insight into a new way of understanding privacy,[78] the thesis suggests that privacy be conceived as: an enabling and positive value – because it nurtures people (individuals and groups). Thus conceived, it occupies both spatial and informational spheres of our lives and allows individuals to obtain a sense of real and/or imagined freedom (rights) to socially construct private and public spheres and allows limited control of: personal information, spatial integrity, reputation, relationships (intimacy), identity (sense of self, self-worth and esteem), and other important human activities within a particular society. Thus privacy also provides the legitimising force behind the issue of personal control, whether or not the force is

---

[77] See Review Panel, Richard Royle, Steve Hambelton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013). This review recommends that as from 1 January 2015 that PCEHR enrolment by consumers should be changed from 'opt-in' to 'opt-out' (Rec.13) and from *consumer-control* to private sector/industry control (amongst other changes). However, at time of writing the date recommended for implementation of these changes (1 January 2015) has passed without these recommendations being embraced by the federal Coalition Liberal Government; see also chapter 7, pp250-255 for discussion of *Royle Review* recommendations.

[78] See, for example, Graeme Laurie, *Genetic Privacy*, above n50 [Laurie contributes to the international genetic privacy debate through analysis of privacy concepts]. His theoretical analysis focuses on the problem of defining privacy, evaluating privacy law discourse, as well as highlighting legal and ethical challenges associated with genetic information in a digital world. Laurie contends that individual human rights focus is inadequate in light of advancing familial genetic information possibilities: at 4. Laurie concludes his analysis by outlining a new privacy paradigm and proposing a definition that would support privacy and public interests: at 245.

expressed as a legal or ethical obligation, or as a 'constructed process'. A 'constructed process' is conceived as capturing those current and future forces that are outside mainstream considerations and are yet to be defined in our society as a force influencing privacy. For example, a 'constructed process' would include the introduction of a *Council* that enhances democratic and individual privacy rights, as well as something (innovative or novel) that is yet to be recognised (invented) such as smart privacy software or systems programs.

III. PRIVACY ─ A NEW UNDERSTANDING

The 21st century has witnessed the emergence of a new breed of international techno savvy privacy scholars.[79] These scholars capture the broader theories associated with global technology, information economy and privacy.[80] For instance the impact of modern technology on privacy is examined in *Technology and Privacy: The New Landscape,*[81] where the authors entertain the question of privacy and its continuing relevance to the modern digital information era.[82] In *Delete* and *Big Data* Mayer-Schonberger explores the phenomenon of data collection and linkage and perfect remembering in the digital age and its relationship with privacy he reveals why we

[79] See, eg, Viktor Mayer-Schonberger, Tal Zarsky, Daniel Solove, Jaron Lanier, Marc Rotenberg, Philip Agre, and Evgeny Morozov.

[80] Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009); Evgeny Morozov, *The Real Privacy Problem*, above n1; Evgeny Morozov, *The Net Delusion: How Not to Liberate* the *World* (book.google.com. 2011); Tal Zarsky, "Mine Your Own Business!": Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion" (2013) 5 *Yale Journal of Law and Technology* 1; Jaron Lanier, *Who Owns the Future?* (Penguin Books, 2013); Spiros Simitis, 'Privacy Lecture' (Paper Presented at Berkeley University Law School, Berkeley California USA, April 2010); Spiros Simitis, "Reviewing Privacy in an Information Society" (1987) *University of Pennsylvania Law Review*; Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" (1994) *Iowa Law Review*.

[81] Agre and Rotenberg, *Technology and Privacy: The New Landscape*, above n1.

[82] See also Subramanian and Katz, *The Global Flow of Information*, above n1.

must reintroduce our capacity to forget.[83] He argues that the digital realm remembers what is sometimes better forgotten and this has profound implications, noting that humiliating content on Facebook is enshrined in cyber-space and potentially in longitudinal *EPR* profiles for future employers and others to see.[84]

Morozov and Zarsky contend that the concept of privacy needs to be considered in a very different light in the modern global technological environment, embracing a wider political agenda. They argue that the modern day concept of privacy in a global world is far more complex than originally conceived by earlier 20th century privacy theorists and has moved beyond the narrow individual information control question to encompass political questions such as public participation and democracy. Both theorists articulate the notion that in order to evolve socially humans require a certain amount of disorder in their lives and that removing the need to exercise individual choice and responsibility will result in citizen political complacency that potentially threatens the very essence of democratic government.[85]

The overarching question that emerges from the above privacy analysis is whether privacy can be conceptualised in light of new technological advances? Any attempt to locate a common denominator for all the manifest things that fall under the

---

[83] Viktor Mayer-Schonberger, *Delete,* above n80*;* Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data* (Harcourt, 2013).

[84] See Bridie Jabour, 'Australian Authors Join Call for UN Bill of Digital Rights to Protect Privacy' *The Guardian* (UK), 10 December 2013, 1; Daily Telegraph, 'Threat to Privacy in E-Health Records' *The Daily Telegraph* (Australia), 28 August 2012, 12; see Danuta Mendelson, "Electronic Medical Records: Perils of Outsourcing and the *Privacy Act* 1988" (2004) 12 *Journal of Law and Medicine* 8; Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for Asia-Pacific' in Kenyon and Richardson, *New Dimensions in Privacy Law*, above n1: at 91; see generally Anne Mainsbridge, "Employers and Genetic Information: A New Frontier for Discrimination" (2002) 2 *Macquarie Law Journal* 61.

[85] See Evgeny Morozov, "The Real Privacy Problem", above n1: at 33; see also Kenyon and Richardson, *New Dimensions in Privacy Law,* above n1. ,

rubric of privacy is an onerous task given the changing social, economic and political environment that exists. Because of these difficulties, some theorists argue that privacy is 'reducible' to other conceptions and rights.[86]

However the thesis argues that privacy issues are far too multifarious to be reduced to rights over the person or property; for example, much insight can be gained from electronic surveillance or conflicts between considerations of privacy and free press rights.[87] It is contended that privacy must be understood as a broader and increasingly essential human right that not only protects human identity but more importantly democratic ideals. Additionally there is a danger of being seduced by outmoded concepts that represent computer utility and neutrality as benign tools of human utility and convenience in light of mounting evidence that technologies are increasingly concerned with economic and social control by governments and information technology organisations such as Google and Facebook.[88] Information technology is essential to bureaucratic government programs such as delivery systems for primary, secondary and tertiary healthcare because the information collected is capable of reporting upon, motivating and shaping individual reactions and controlling behaviour of individuals and communities.[89]

---

[86] See Daniel Solove, *Understanding Privacy*, above n4: at 37; Judith Thompson, 'The Right to Privacy' in Ferdinand Schoeman, *Philosophical Dimensions of Privacy: An Anthology,* above n44: at 272. Judith Thompson argues that the 'right to privacy is not a distinct cluster of rights but itself intersects with the cluster of rights which the right over the person consists in and also with the cluster of rights which owning property consists in': at 280.

[87] See chapter 1, pp1-37; chapter 7, pp238-261.

[88] See ALRC, *Serious Invasions of Privacy in the Digital Era*: Discussion Paper 80 (31 March 2014); see also *The Coalition's Policy on E-Government for the Digital Economy* (September 2013).

[89] Evgeny Morozov, "The Real Privacy Problem", above n1; Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep-up with Technology Changes", above n3; see also Carol Grbich, 'Moving Away from the Welfare State: The Privatisation of the Health System' in Heather Gardiner and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2002).

The disadvantage for individuals in this situation is the danger of becoming complacent in the privacy debate and no longer questioning the motives of governments and architects of social technologies as society moves to embrace constructed cyber-space reality and the digital person. Thus it is imperative in the *EPR* and e-health implementation privacy debate to conceptualise privacy as not just an individual's right to control personal information in the new information age but see privacy as a right that is increasingly essential to protecting broader democratic rights. The introduction of a *Council* as proposed by the thesis is a significant step towards inclusively engaging the general public in the healthcare privacy protection debate. Also a *Council* represents a participatory social mechanism that further supports the government's legal, governance and technological privacy protection schemes.

IV. CONCLUSION

In summary, the above exploration of privacy discourse does provide valuable insight into the 'evolving' modern day concept of privacy. Nevertheless, these stand-alone theories still fail to adequately explain the multidimensional character of privacy in the modern technology information era. Prior to 1990s, privacy violations had been understood in a particular manner[90] and it was only when these more customary ways of understanding privacy did not account for key aspects of the unique problems associated with the digital age that privacy theory moved beyond individual rights

[90] See Warren and Brandeis, "The Right to Privacy", above n11; see also Brett Mason, *Privacy without Principle*, above n6 [according to Mason 'before electronic information became common place-privacy was traditionally considered to include a person's private personal details such as name, occupation, address and date of birth']: at 10.

concerns. Particularly evident during this period is the rise of computers, which made privacy erupt into a frontline issue around the world.[91] Consequently privacy rights no longer focus on an individual's right to control information at a community level or maybe even at the national level, the digital age demands that the world is now viewed through global eyes:

> The proliferation of communication technology has advanced at an unprecedented speed. In the first decade of the 21st century the number of people connected to the Internet increased from 350 million to more than 2 billion…By 2015, the majority of the world's population will, in one generation, have gone from having no access to unfiltered information to accessing all of the world's information through a device that fits in the palm of their hand. If the current pace of technological innovations is maintained, most of the projected eight billion people on Earth will be online.[92]

Privacy theory discourse highlights major concerns relating to the problem of adequately capturing the multidimensional meaning of privacy. Privacy scholars in Australia and internationally continue to struggle with trying to define privacy and protect individual privacy, particularly in the present global context. However a common denominator in privacy discourse includes the transformational power of technologies to drive privacy protection, the continuous reliance on 'free flow' information, and problems such as fear and surveillance associated with the ongoing 'war on terror'.[93]

A further privacy concern includes the recognition of privacy as a human condition that helps develop and sustain the concept of 'self' as separate and unique, and its role in controlling the 'unwanted gaze' of others, particularly in a world that seeks to amplify and objectify encounters with it.[94] Personal healthcare information

---

[91] See chapter 3, pp70-98 detailing the evolution of technology.

[92] See Eric Schmidt and Jared Cohen, *The New Digital Age* (John Murray, 2013) 4.

[93] See chapter 3, pp70-98 for discussion on transformational power of modern technologies.

[94] Ibid.

no longer enjoys a quasi 'quarantined' privacy status, as the 'value' of all information is fully realised and 'pursued by capitalism and bureaucratic administration.'[95]

In time some of these more pressing privacy questions will be resolved. Nevertheless it is how societies like Australia view the true social value of privacy and privacy protection that remains important to the continuing privacy debate in the modern world. Because if privacy is a concept that is valued by the majority of citizens then it stands to reason that it will be considered important enough and adequately protected. On the other-hand if it is perceived as an impediment of some kind, to say economic and technological advancement and progress, privacy rights may be in danger of being subsumed by advancing collective interests and maybe even be lost. Privacy is ultimately about 'rights' and how those rights are advanced, protected or compromised.

The following chapter 5 progresses the thesis argument that the Australian Government needs to do more in order to adequately protect individual healthcare privacy in light of e-health development. It does this by exploring the federal Government's plan to introduce new legal, governance and technological measures to ensure the protection of Australian privacy rights in the new electronic healthcare regime.

---

[95] See Evgeny Morozov, "The Real Privacy Problem", above n1 [Morozov contends that as web companies and government respond to ever more information needs, 'it is tempting to respond by passing new privacy laws or creating mechanisms that pay us for data']: at 1. Instead of passing new privacy laws, Morozov argues that what we need is privacy solutions that recognise the political agenda of the privacy debate and do not put democracy at risk: at 1; see also Martha Nussbaum, *Not for Profit: Why Democracy Needs the Humanities* (Princeton University Press, 2010); see also chapters 1, pp1-37; chapter 3, pp70-98; chapter 6, pp184-237; , chapter 7, pp238-261- for further thesis details and discussion on privacy risks.

CHAPTER 5

SHORTCOMINGS OF COMMON LAW AND STATUTORY LAW IN THE PROTECTION OF INDIVIDUAL PRIVACY RIGHTS

Laws which govern all aspects of life in Australia, including health and privacy areas are enacted by Parliament (State and Commonwealth) according to the distribution of legislative powers in the *Commonwealth Constitution*.[1] In addition to statutes, there exists in Australia 'judge-made' or 'common law,' as well as international obligations, which impacts on modern health and privacy law. This chapter explores the evolution of Australian health, e-health and privacy law. It also highlights the growing significance of law in the modern digital economy era, arguing that law, despite its deficits, remains a vital mechanism for protecting human rights privacy and directing Australian health reform.

The Australian health system 'is a product of a diverse range of economic, technical, social, legal, constitutional and political factors, some of which are unique to Australia.'[2] The health system is also a product of the historical evolution from the

[1] *Commonwealth of Australia Constitution Act* 100 (Imp); see John Devereux, *Australian Medical Law* (Routledge-Cavendish, 3rd ed, 2007). The Commonwealth of Australia was formed in 1901. The new Commonwealth (Federal) Parliament was assigned powers in respect of certain prescribed areas. Devereux argues that in order to understand the regulations of the delivery of health services in Australia then, recourse must first be had to the *Constitution*: at 117-119.

[2] K Wheelwright, "Commonwealth and State Powers in Health — A Constitutional Diagnosis" (1995) 21 (1) *Monash University Law Review* 53: at 53, 55, 82-83.

provision of care based on private philanthropy to a system which is largely government funded and controlled. The way health services are organised, funded and delivered is affected by the existence of federalism as a major organising principle for the distribution of power in Australia.[3]

I. FEDERALISM – CONSTITUTIONAL FRAMEWORK

In the late 19th century, the framers of the *Constitution* chose federalism as the preferred model for establishing the new Commonwealth Government. Federalism is described as a 'two-tiered system of government in which the power is divided between the central and State or regional Government.'[4] The degree of diversification of powers between State/Territory/Province and central Government may vary between different countries, such as the United States (U.S.) and Canada. The Australian experience of federalism closely approximated that of the U.S. Australian federalism was also deeply influenced by its British heritage and Westminster tradition of 'responsible government'.[5] The main issues facing the framers of the *Constitution* were how to reconcile national unity with the maintenance of 'state rights', and how best

[3] K Wheelwright, "Commonwealth and State Powers in Health", above n2; see John Devereux, *Australian Medical Law*, above n1: at 118.

[4] Greg Taylor, "Federalism in Australia" [2010] *Monash University Law Research Series* 11; Martin Painter, *Collaborative Federalism: Economic Reform in Australia in the 1990s* (Cambridge University Press, 1998); Frank McGrath, *Framers of the Australian Constitution: 1891 – 1897 Their Intentions* (Frank McGrath Publisher, 2003).

[5] Frank McGrath, *The Framers of the Australian Constitution*, above n4: at 31; Tony Blackshield and George Williams, *Australian Constitutional Law and Theory* (The Federation Press, 5th ed, 2010) 35; see also Justice John Toohey, "A Government of Laws, and Not of Men?" (1993) 4 *Public Law Review* 158.

to balance the power between the smaller and larger states of the Commonwealth.[6]

Additionally federation was to 'harmonise' a combination of local powers with local autonomy – 'Our Australian concert is not one of unison, but of harmony, in which the difference of each part blends together in forming the concord as a whole.'[7] Nevertheless, despite the founder's earlier vision, over the years since the commencement of the Commonwealth there has been a gradual increase in Commonwealth control over the whole Australian economy.[8] This occurred as a result of constitutional changes validating the inter-governmental Financial Agreement resulting from the Great Depression, and the Commonwealth take-over of the power to levy income tax from the States, as well as centralist interpretations of the *Constitution* favouring an increase in the economic power of the Commonwealth.[9]

---

[6] See Justice John Toohey, "A Government of Laws, and Not of Men?", above n5: at 31; Frank McGrath, *The Framers of the Australian Constitution*, above n4: at 10-51; Clement MacIntyre and John Williams (eds), *Peace, Order and Good Government* (Wakefield Press, 2003); *Australia Act 1986*, s2(2) ['It is hereby further declared and enacted that the legislative powers of Parliament of each State include all legislative powers … for the peace, order and good government of that State'].

[7] Frank McGrath, *The Framers of the Australian Constitution*, above n4, cites Dr Cockburn (South Australia): at 17.

[8] Martin Painter, *Collaborative Federalism,* above n4.

[9] Martin Painter, *Collaborative Federalism*, above n4; see Blackshield and Williams, *Australian Constitutional Law and Theory*, above n5. During the World War 11, the Commonwealth passed four Acts (*Income Tax Act* 1942 (Cth); *States Grants (Income Tax Reimbursement) Act* 1942 (Cth); *Income Tax (War-time Arrangements) Act* 1942 (Cth); *Income Tax Assessment Act* 1942 (Cth)), which forced the States to relinquish their income tax powers: at 205. The validity of the tax arrangement was upheld in *South Australia v Commonwealth* (First Uniform Tax Case) (1942) 65 CLR 373 and reaffirmed in *Victoria v Commonwealth* (Second Uniform Tax Case) (1957) 99 CLR 575. See also J A La Nauze (ed), *Federated Australia: Selections from Letters to the Morning Post 1900-1910* (Melbourne University Press, 1968). The Uniform Taxes Cases bore out the prophecy of Alfred Deakin, that the States would find themselves 'legally free, but financially bound to the chariot wheels of the Central Government': at 97.

The State governments' powers to make laws are deemed limited only by the narrowly defined powers of the federal government as set out in the *Constitution*. Section 107 of the *Constitution* provides that every power the State government had prior to Federation was to remain vested in them unless 'it is by this Constitution exclusively vested in the Parliament of the Commonwealth or withdrawn from the Parliament of the State'.

Under this arrangement, the Commonwealth can only exercise those 'enumerate' powers conferred upon it by the *Constitution* – including the 'incidental' power under s51(xxxix), which permits the Commonwealth to make laws with respect to matters 'incidental' to any 'enumerate' powers. The specified, 'listed' Commonwealth powers are, with a few exceptions, 'concurrent' powers and are set out in s51. Because these powers are concurrent, the States may make laws in these areas as well as the Commonwealth,[10] subject to s 109 inconsistency.

The potential of existence of both federal and State laws on certain issues introduces the possibility of conflict between the laws as stated by each piece of legislation. Section 109 of the *Constitution* provides that where both state and federal legislation exits, and there is inconsistency between the laws, Commonwealth law applies, and the State law is rendered invalid.[11] If a state

---

[10] By virtue of s122 of the *Constitution*, the Commonwealth has a broad power to pass laws on any subject in relation to the Australian Territories.

[11] *Commonwealth Constitution*, s51 – there are 39 placita (decrees) in that section. These include such matters as trade and commerce with other countries, for example, 'external affairs' (pl xxix); nationalisation and aliens (pl xix); corporation (pl xx); quarantine (pl ix); taxation (pl ii); marriage (pl xxi); and divorce and matrimonial causes (pl xxii).

chooses to refer one of its powers to the federal government, then the federal government can legislate on the matter.[12] Additionally s128 requires an amendment to be passed by a referendum carried by the popular vote in a majority of states before the *Constitution* can be changed or amended. As a consequence very few constitutional referendums have ever been successful; thus the *Constitution* remains relatively unchanged since its inception.[13]

Also under s51 (xxix) the Commonwealth has the power to make laws in respect of 'external affairs'. This power enables the Commonwealth to implement obligations under 'bona fide treaties'.[14] However, the question has been robustly debated as to whether the mere entry of the Executive into an international Treaty, Agreement, or Convention, automatically gives the Commonwealth Parliament the power to legislate on the subject matter of such an instrument, in cases where the Commonwealth Parliament has otherwise no specific power so to legislate.[15] Thus,

---

[12] *Commonwealth Constitution* s51(xxxvii) provides that the federal Parliament may validly pass laws on any matter referred to it by a State Parliament, even if it would otherwise lack the capacity to legislate on that subject.

[13] Section 128 of the *Constitution* incorporates the referenda mechanism, by which it can be altered. Since 1901, 44 proposals have been put to the people, with only eight succeeding. Thus, the *Constitution* stands largely as it did in 1901. See also Justice John Toohey, "A Government of Laws, and Not of Men?" above n5: at 158.

[14] See, for example, World Health Organisation ('WHO'), *International Health Regulations 2005*, Art 2, reproduced in *International Health Regulations* (World Health Organization, 2nd ed, 2008) incorporated into Australian law by the *National Security Act 2007* (Cth); United Nation ('UN'), *International Covenant on Civil and Political Rights* ('ICCPR') 16 December 1966, [1980] ATS 23 (entered into force on 23 March 1976). Article 17 of the *ICCPR* provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, correspondence, nor to unlawful attacks on his honour or reputation' ratified in Australia on 13 August 1980.

[15] See Hiliary Charlesworth, Madelaine Chiam, Devika Hovell and George Williams, "Deep Anxieties: Australia and the International Legal Order" (2003) 25 *Sydney Law Review* 423; see also Frank McGrath, *The Framers of the Australian Constitution*, above n4: at 249; The *Commonwealth v Tasmania* ('Tasmanian Dam Case') (1983) 158 CLR 1. In the *Tasmanian Dam Case*, Mason J touched upon the possible effect that the wide interpretation of the 'external affairs' power (s51 (xxix)) might have on the relationship between the Commonwealth and the States.

despite the international legal framework of the right to the 'highest attainable standard of health', which is central to many international conventions to which Australia is a signatory, there are no guarantees that the Australian government will legislate for compliance domestically, in accordance with its international obligations.[16]

The *Constitution* gives no explicit power over health to the Commonwealth Parliament. Some powers over these matters, however, inferentially lead to the Commonwealth Parliament having control over health-related matters. This occurs because s51 (xxxix) allows the federal Parliament to pass legislation concerning matters ancillary to areas of federal legislative competence, for instance, s51 (xxiii) – invalid [disability] and old age pensions.[17] In 1943 the federal Government attempted to introduce a scheme of pharmaceutical benefits. The *Pharmaceutical Benefits Act 1944* (Cth) provided for the gratuitous provision of the public of certain medicines, it also imposed duties on Medical Practitioners and Pharmacists in relation to the prescription and supply of medicines. In passing the Act the Commonwealth relied upon s81 of the *Constitution* which permits the Commonwealth 'to make

---

[16] See *Chow Hung Ching v The King* (1948) 77 CLR 449 per Dixon J: at 478. In this case Dixon J emphasised 'that the executive action of ratifying a treaty, thus committing Australia to it internationally, is effective only externally'; see generally *Workplace Relations Amendment (Work Choices) Act 2005* (Cth) ('*Work Choices*'). Despite being concerned with Industrial Law this case provides a clear example of how the Government failed to protect fundamental workplace human rights standards, including 'rights of association' and 'collective bargaining' obligations: at 9. At the time the federal Liberal Coalition Government chose to ignore international criticism about breaches of 'standards' and also refused to remedy the situation.

[17] See generally, *National Health Act 1953* (Cth) ss85-105; *National Health (Pharmaceutical Benefits) Regulations 1960* (Cth); *Pharmaceutical Benefits Act 1947* (Cth) - the Pharmaceutical Benefits Scheme (PBS) is a federal Government scheme operated under s51 (xxiiiA) of the *Constitution*, this scheme allows the Australian population to access a large range of prescription drugs at low cost. It originally formed part of general social welfare legislation that followed *World War II*; see also Financial and Analysis Branch Commonwealth Department of Health and Aged Care, *The Australian Health Care System: An Outline* (September 2000).

appropriations for the purposes of the Commonwealth'.[18] The absence of clear legislative authority residing in the *Constitution* resulted in the State of Victoria opposing the legislation and claiming that s81 should be construed as only meaning purposes for which the Commonwealth Parliament has power to make laws under the numerous subsections of s51 of the *Constitution*.

The majority of the High Court in *Attorney General for Victoria (ex rel Dale and Ors) v Commonwealth and Ors* (1945) (*Pharmaceutical Benefits Case)*[19] held that the *Pharmaceutical Benefits Act 1944* (Cth), which provided for specified pharmaceutical benefits to be payable out of the trust account established under the *National Welfare Fund Act* 1943 (Cth), was ultra vires and therefore invalid.[20] Mr Justice Williams' decision clearly articulated his condemnation of the federal Government's interference with health issues:

> [The *Pharmaceutical Benefits Act 1944*] contains provisions affecting the relationship, contractual or under the laws of the State, of medical practitioners and patients, of customers and chemists … There is no express power under the Constitution for the Parliament of the Commonwealth to legislate upon this subject matter except to make laws with respect to quarantine and as incidental to the execution of any powers vested in the Commonwealth by the Constitution.[21]

---

[18] See, *Williams v Commonwealth of Australia* [2012] HCA 23 (20 June 2012) (No 1); *Williams v Commonwealth of Australia* [2014] HCA 23 (19 June 2014) (No 2). The questions of Executive power of the Commonwealth under funding and appropriation remains a current issue in Australia. The *William's* case examined whether the law providing for payments in circumstances identical to the Funding Agreement would be law with respect to s51 (xx) and s51 (xxiiiA) of the *Constitution*. It was held by the Court that the making of payments by the Commonwealth was beyond the executive power in s61 of the Commonwealth.

[19] *Attorney General for Victoria (ex rel Dale and Ors) v Commonwealth and Ors* (1945) 71 CLR 237 (*The Pharmaceutical Benefits Case*); see also Gerard Carney, *The Constitutional Systems of the Australian States and Territories* (Cambridge University Press, 2006) 393; McIntyre and Williams, *Peace, Order and* Good *Government,* above n6: at 10.

[20] See particularly, the challenge on the meaning of 'the purposes of the Commonwealth' in the *Pharmaceutical Benefits Case* (1945) 71 CLR 237; [1945] HCA 30. However, the *Pharmaceutical Benefits Case* yielded no majority view on the constitutional 'limits' of 'the purpose' of this meaning. McTiernan J agreed with Latham CJ, holding that 'the purposes of the Commonwealth are … as Parliament determines': at 273. Dixon J, with whom Rich J agreed, took a narrower view, but held the Act was invalid: at 268. Starke and Williams JJ adopted a narrower view and held the Act invalid: at 282.

[21] *The Pharmaceutical Benefits Case* (1945) 71 CLR 237 per Mr Justice Williams: at 280.

As a result the scope of the Social Security power the *Constitution* was enlarged by way of Constitutional Referendum in 1946. By adding the new s51 (xxiiiA) to the *Constitution* this gave the Parliament power to legislate with respect to:

> The provision of maternity allowances, widows' pensions, child endowment, unemployment, pharmaceutical, sickness and hospital benefit, medical and dental services (but not so as to authorize any form of civil conscription), benefits to students and family allowances.

The federal Government again enacted a *Pharmaceutical Benefits Act 1947* (Cth) along similar lines to the 1944 Act. Section 7A of the new 1947 Act provided that a Medical Practitioner could not provide medicines or appliances in the formulary or addendum except by using a form prescribed by the Commonwealth. A penalty was provided for non-compliance. The British Medical Association in Australia challenged the legislation on the basis it contravened the express words of s51 (xxiiiA) of the *Constitution*:[22]

> [W]henever medical or dental services are provided pursuant to a law with respect to the provision of some benefit, eg, sickness or hospital benefits, 'the law must not authorise any form of civil conscription of such services …..'[23]

The extent of the protection which these words gave to healthcare professionals was illustrated by the High Court's decision in *British Medical Association v Commonwealth* (1949).[24] In this case a majority of the court decided that s7A of the *Pharmaceutical Benefits Act 1946* (Cth) infringed the prohibition on civil conscription in that it obliged a medical practitioner to use a form supplied by the Commonwealth.[25] However, in

---

[22] *Federal Council of the British Medical Association in Australia and Ors v The Commonwealth and Ors* (1949) 79 CLR 201.

[23] *British Medical Association v Commonwealth* (1949) 79 CLR 201 per Williams J: at 286-287. See also *Alexandra Private Geriatric Hospital Pty Ltd v Commonwealth* (1987) 162 CLR 271, 279.

[24] *British Medical Association v Commonwealth* (1949) 79 CLR 201.

[25] Latham CJ, Rich, Williams and Webb JJ; Dixon and McTiernan JJ dissenting.

1980 the High Court qualified this expansive reading of the prohibition on civil conscription. In *General Practitioners Society of Australia v Commonwealth* (1980),[26] the court said that the clause prohibited:

> Any sort of compulsion to engage in practice as a doctor or dentist or to perform particular medical or dental services. However, in its natural meaning it does not refer to compulsion to do, in a particular way, some act in the course of carrying on practice or performing a service, when there is no compulsion to carry on this practice or perform the service.[27]

It held that Commonwealth legislation could compel any Medical Practitioner, who delivered a medical service, which was to be financed by the Commonwealth to deliver that service in accordance with a government specified procedure.

As long ago observed by Hanks, 'while this approach favours more scope for Commonwealth regulations of incidents of medical and dental practice, the extent of that regulation remains constrained'[28] by a number of other propositions such as that it does not give the Commonwealth direct power to regulate the delivery of health services through the private sector. Dixon J made the observation in *British Medical Association v Commonwealth,*[29] that '[t]he purpose of the constitutional amendment was to enable the Commonwealth to provide the … services which para (xxiiiA) mentions.'[30] Despite these limits it seems that the Commonwealth Parliament can

---

[26] *General Practitioners Society of Australia v Commonwealth* (1980) 145 CLR 532 per Latham CJ and Webb J '[F]or all the above reasons, none of the provisions in question imposes any form of conscription contrary to s51 (xxiiiA) of the Constitution': at 532. See also Danuta Mendelson, "Devaluation of a Constitutional Guarantee: The History of Section 51 (xxiiiA) of the Commonwealth Constitution" [1999] *Melbourne University Law Review* 14 [this article describes constitutional and socio-historical background to the referendum that led to the insertion of s51 (xxiiiA) into the Commonwealth Constitution].

[27] *General Practitioners Society of Australia v Commonwealth* (1980) 145 CLR 532, per Gibbs J: at 557.

[28] P J Hanks, *Constitutional Law in Australia* (Butterworths, 1991) 372; see also Jennifer Clarke, Patrick Keyzer, James Stellios and John Trone, *Hanks Australian Constitution Law: Material and Commentary* (LexisNexis, 9th ed, 2012).

[29] *British Medical Association v Commonwealth* (1949) 79 CLR 201.

[30] *British Medical Association v Commonwealth* (1949) 79 CLR 201 per Dixon J: at 260.

impose regulations on those healthcare providers who choose to participate in Commonwealth-funded healthcare programs. For example, it appears that Medical Practitioners who deliver Commonwealth funded services can be required to furnish accurate information to the Commonwealth's Health Insurance Commission; they can be required to charge consumers in accordance with a schedule of prescribed fees; and they can be prohibited from using pathology services in which they hold financial interest.'[31]

The appropriation and grants powers found in s81 and s96 has provided the constitutional foundation for welfare services programs extending beyond the area of healthcare provision. For instance, the Australian Assistance Plan provided Commonwealth funds to support the development of community-based welfare programs across a diverse range of activities. The Australian Assistance Plan (AAP) and its validity was considered in *Victoria v Commonwealth* (1975).[32] Thus the broad interpretation of the case to the Commonwealth's use of s81, confirmed by Mason CJ, Deane and Gauldron JJ in *Davies v Commonwealth* (1988), implies 'that the Commonwealth Parliament could rely on the section to provide the constitutional basis for welfare service delivery programs in areas such as child care, legal aid and public housing.' [33] It is also possible for the Commonwealth Parliament with the cooperation of the States (s96) 'to support tied grants of "financial assistance" to the

[31] See *Health Insurance Act 1973* (Cth) ss10, 11; s20B; Pt 11A; see generally *Private Health Insurance Act 2007* (Cth); see also P J Hanks, *Constitutional Law in Australia*, above n28: at 371-372.

[32] *Victoria v Commonwealth* (1975) 134 CLR 338.

[33] *Davies v Commonwealth* (1988) 166 CLR 79: at 96.

States—grants which tied to specific purposes are nominated by the Commonwealth Parliament.'[34]

The *National Health Act 1953* (Cth) and the *Health Insurance Act 1973* (Cth) represent the two most significant pieces of Commonwealth legislation in the health care field. The *Health Care Act*, in addition to allowing for the provision of a wide range of health services, provides conditions for receipt for health care in nursing homes, regulates the establishment of business of organisations providing medical and hospital benefits and provides for and regulates the payment of benefits for pharmaceuticals prescribed by Medical Practitioners. Pursuant to s51 (xxiiiA) and s96 of the *Constitution*, in 1984 the Commonwealth introduced Medibank, a universal scheme of health insurance now known as Medicare.[35]

As outlined by the above analysis of Commonwealth Parliament regulatory powers in respect of healthcare, the balance of powers repose in the State Governments in Australia. Under s96 of the *Constitution*, the federal Government is empowered to make grants to the States 'on such terms as it sees fit'. In practice, since the federal Government collects all the income tax in Australia, this gives the federal Government enormous leverage power to determine the scope of healthcare. This practice can be evidenced by the federal Government funding the provision of

---

[34] See *Williams v Commonwealth of Australia* (No 1) [2012] HCA 23 and *Williams v Commonwealth of Australia* (No 2) [2014] HCA 23.

[35] See *Health Services (Medicare) Act 1973* (Cth). The earlier Medibank program is now known as the Medicare program (see fn33, chapter 2). Funding for Medicare and other healthcare projects is negotiated between the Commonwealth and the States under the *States (Tax Sharing and Health Grants) Act 1981* (Cth). Agreements between the Commonwealth and the States are incorporated in the *Health Insurance Act 1973* (Cth), schedule 2; *Health (Amendment) Act 1994* (ACT); *Private Health Insurance Act 2007* (Cth); *Health Administration Act 1982* (NSW); *Medicare Principles and Commitments Act 1994* (Qld); *Health (Regional Boards) Amendment (Medicare Agreement) Act 1993* (Tas); *Health Services Act 1988* (Vic).

hospitals in the States in return for certain undertakings by the States (e.g. Medicare agreements). Consequently, Australian States have regulated by means of legislation, various aspects of health including access to patient records and patient complaints mechanisms, discussed later in the chapter.

II. LIMITATIONS OF THE CONSTITUTION

A. *Bill of Rights*

Despite embracing the U.S. constitutional model, the *Constitution* does not include a constitutional Bill of Rights and does not have an expressed 'rights' guarantee within the *Constitution*.[36] This situation potentially complicates the question of human rights protection, such as privacy protection in contemporary society, because having a 'written' guarantee of rights embedded within the *Constitution* would provide an extra specific layer of important human rights protection mechanisms (such as privacy) that would be harder for any government in power to dismiss, ignore or override.[37]

---

[36] See Martin Flynn, Sam Garkawa and Yvette Holt, *Human Rights: Treaties, Statutes and Cases* (LexisNexis, 2011). The Constitution of the United States (1789), Bill of Rights (1791) model undermines the concept of parliamentary sovereignty. 'The conventions of a number of the States having at the time of their adopting the Constitution, expressed desire, in order to prevent misconstruction or abuse of powers, that further declaratory and restrictive clauses should be added': at 500; see also Bill of Rights Amendment I, II, III.

[37] See George Williams, *Human Rights under the Australian Constitution* (Oxford University Press, 1999): at 46. For example, the model used for *Charter of Human Rights and Responsibilities Act 2006* (Vic), the *Human Rights Act 2004* (ACT) and other common law models can be overridden by Parliament, unlike the U.S. model; Office of the High Commissioner for Human Rights, *Training Manual on Human Rights Monitoring* (2001). The *Training Manual* refers to human rights as: 'Human Rights are universal legal guarantees protecting individuals and groups against actions by governments which interfere with fundamental freedoms and human dignity. Human rights law obliges governments to do some things, and prevents them from doing others': at Chapter 1 (extract) full text published at University of Minnesota Human Rights Library http://humanrights.law.monash.edu.au/monitoring-training.html (viewed 12/11/2012).

The absence of a 'written' guarantee of rights (outside the jurisdictions of Victoria and the Australian Capital Territory discussed below) does not imply that the common law (and any international treaty protections enacted in domestic law) does not provide important protections in addition to statutory protections in the area. What it suggests is that modern-day reliance on 'honourable men in a civilised society',[38] adherence to Parliamentary Sovereignty, common law, administrative law and international instruments in Australia may not prove robust enough, and thus may fail to fully deliver the necessary protection of individual privacy rights and protection required in the modern information economy.[39]

Since the 1970s, alongside judicial considerations, other areas of review, such as in the context of administrative law, have developed in an attempt to deal with the absence of constitutional guarantees in human rights claims.[40] It is recognised that public officials and government agencies possess wide and often discretionary powers which profoundly affect the rights and liberties of

---

[38] Geoffrey de Q Walker, "Dicey's Dubious Dogma of Parliamentary Sovereignty" (1985) 59 *Australian Law Journal* 276 in Blackshield and Williams, *Australian Constitutional Law and Theory*, above n5: at 102. According to Walker, the picture of British constitutionalism presented in the late 19th century by A V Dicey (1835-1922) proved extremely influential in Australia: at 102. Dicey argued that the fundamental principles of British constitutional law were representative democracy, parliamentary sovereignty and the rule of law: at 100; see George Williams, *Human Rights under the Australian Constitution*, above n38. Williams' provides an analysis of common law and international law human rights development, also asks is statute law a de facto Bill of Rights?: at 10-23.

[39] See Lyria Bennett Moses, "Recurring Dilemmas: The Law's Race to Keep Up With Technological Change" [2007] *University of New South Wales Law Research Series* 21: at 1; see also George Williams, *Human Rights under the Australian Constitution*, above n38: at 47; Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Routledge, 2006); see also Dan Jerker B Svantesson, "Privacy, The Internet and Transborder Data Flows: An Australian Perspective" (2007) 19 *Bond Law Review* 1.

[40] Ben Saul, 'Australian Administrative Law: The Human Rights Dimension' in Matthew Groves and H P Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007): at 50.

people in Australia.[41] On an abstract level, some consonance exists in fundamental values underpinning human rights law and administrative law, as both systems of law aim to restrain arbitrary or unreasonable government action and help to protect the rights of individuals.[42] Similarly, they share a concern for fair and transparent process, the availability of review of certain decisions and the provision of effective remedies for breaches of the law.[43]

A defining feature of Australian administrative law is the important role played by non-judicial bodies, such as tribunals and the Commonwealth and various state and territory ombudsman, in relation to complaints about the actions of agencies of the executive government (ministers, departments, agencies and individual officials who work within these bodies).[44] However, the limitations of human rights and administrative law have traditionally been primarily directed towards controlling 'public' power rather than interfering in the 'private' realm.[45]

---

[41] Groves and Lee, 'Australian Administrative Law: The Constitutional Matrix' in Matthew Groves, *Australian Administrative Law*, above n40: at 1.

[42] Greg Weeks, 'The Use and Enforcement of Soft Law by Australian Public Authorities' (Paper Presented at the Practice and Theory of Soft Law Academic Symposium, Peking University, 9 July 2011).

[43] Ben Saul, 'Australian Administrative Law: The Human Rights Dimension' in Groves and Lee, *Australian Administrative Law*, above n40: at 51.

[44] See Robin Creyke and John McMillan, *Control of Government Action* (LexisNexis, 3rd ed, 2012) 22; Roger Douglas, *Administrative Law* (LexisNexis, 2nd ed, 2004): at 2, 279.

[45] See Ben Saul, 'Australian Administrative Law' in Groves and Lee, *Australian Administrative Law*, above n40: at 55; Andrew Murray, 'Should States have a Right to Information Privacy?' in Klang and Murray, *Human Rights in the Digital Age*, above n39: at 191; see also Roger Brownsword, 'Biotechnology and Rights: Where are we Coming From and Where are we Going?' in Klang and Lee, *Human Rights in the Digital Age*, above n39: at 219; see generally Huw Beverley-Smith, *The Commercial Appropriation of Personality* (Cambridge University Press, 2002).

In the new digital information economy, given the rapidity of technological change, this privileged view towards the private realm does not necessarily take into account the ever-shifting boundary between the public and private spheres.[46] As the ALRC pointed out in *Serious Invasions of Privacy in the Digital Era and Copyright and the Digital Economy*, there is an urgent need for reform in this area.[47] An additional concern is that, under international human rights treaties, only 'states parties' expressly owe legal obligations to protect rights.[48] As a consequence private persons are not parties to human rights treaties, which do not have 'direct horizontal effects' in international law and are not regarded as substitutes for domestic law.[49]

According to Carney, 'Australia is a parched landscape so far as purchase for a legal form of any right to health is concerned,' which results in

---

[46] ALRC, *Serious Invasions of Privacy in the Digital Era:* Discussion Paper 80 (March 2014). According to the ALRC, Discussion Paper 80 particular attention has been directed to 'the rapidly expanded technological capacity of organisations not only to collect, store and use personal information': at 21-22 and 37-41, but also 'to track the physical location of individuals, to keep activities of individuals under surveillance': at 41-42, 'to collect and use information posted on social media, to intercept and interpret the details of telecommunications and emails': at 40-41, and 'to aggregate, analyse and sell data from many sources': at 21-23; see also ALRC, *Review of Australian Privacy Law:* Discussion Paper 72 (September 2007): at 335-337, 599-610, 667-670; see also Brett Mason, *Privacy without Principle* (Australian Scholarly Publishing, 2006) 9-12.

[47] ALRC, *Serious Invasions of Privacy in the Digital Era*: Issues Paper 43 (2013): at 14; ALRC, *Copyright and the Digital Economy*: Summary Report 122 (2013): at 6.

[48] Martin Dixon, Robert McCorquodale and Sarah Williams, *International Law* (Oxford University Press, 5th ed, 2014); Antonio Cassese, *International Law* (Oxford University Press, 2002) [Cassese recognises sovereign states as the legitimate parties to treaty obligations]: at 46.

[49] Charter of the *United Nations*, opened for signature 26 June 1945, Australian Treaty Series 1945 No 1 (entered into force 24 October 1945, entered into force for Australia 1 November 1945); the *Security Council*; the *Economic and Social Council* (ECOSOC) and the *International Court* of *Justice* Article 92. The UN created the *Commission on Human Rights* in 1946. This body was replaced by the *Human Rights Council* in 2006, by General Assembly Resolution 60/251. Human Rights Committee, *General Comment No 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant* UN DocCCPR/C/21/Rev.1/Add.13,18 (26 May 2004).

a human rights deficit.[50] It has no federal or state Bill of Rights, apart from Victoria and Australian Capital Territory[51] and even these do not extend to socio-economic (so-called 'positive') rights. Adverse rulings can be overridden by state and territory Parliaments.[52] Recent calls for a national Bill of Rights were rejected by government.[53] Instead, a Senate Joint Parliamentary Committee on Human Rights now has power to examine and report on existing or proposed legislation and subordinate legislation (such as statutory regulations and instruments) for human rights compatibility, and human rights assessment must accompany any new Bills or allowable instruments.[54] While the Senate Joint Committee on Human Rights represents a very positive step, it is posited that the lack of an embedded, written, human rights guarantee in Australia leaves its citizens in a vulnerable position[55] as compared

---

[50] Terry Carney, 'Human Rights and Health Law' in Ben White, Fiona McDonald and Lindy Willmott (eds), *Health Law in Australia* (Thomson Reuters, 2nd ed, 2014): at 114; see also Terry Carney "Neoliberal Welfare Reforms and "Rights" Compliance Under Australian Social Security Law" (2006) 12(1) *Australian Journal of Human Rights* 223-255.

[51] See *Human Rights Act 2004* (ACT); *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[52] Terry Carney, "Neoliberal Welfare Reforms", above n50.

[53] See Bryan Horrigan, "Reforming Rights-Based Scrutiny and Interpretation of Legislation" (2012) 37(4) *Alternative Law Journal* 228-232.

[54] See *Human Rights (Parliamentary Scrutiny) Act 2012* (Cth) s 7(a)-(b). The purpose of the *Human Rights (Parliamentary Scrutiny) Act* is to establish a committee on human rights and other related purposes. For example, the Australian Government amendments to the *Personally Controlled Electronic Health Records Act 2012* (Cth) ('PCEHR Act') and *Personally Controlled Health Records (Consequential Amendments) Act 2012* (Cth) 'are compatible with human rights and freedoms, recognised or declared, in the international instruments listed in s 3 of the *Human Rights (Parliamentary Scrutiny) Act*'.

[55] See George Williams, *A Bill of Rights for Australia* (New South Publishing, 2000) [Williams discusses s 51(xxvi) of the *Australian Constitution*, in relation to the ability to pass laws on the topic of any race]: at 2; see also *Kartinyeri v Commonwealth* (1998) 195 CLR 337 ('*Hindmarsh Island Case*') [where the federal Government sought to persuade the High Court of Australia that the Commonwealth had power to pass laws that discriminated against Australians on the basis of their race, in order to pass the *Hindmarsh Island Bridge Act 1997* (Cth) (supported by Northern Territory, South Australia and Western Australia)]. This Act would override the *Aboriginal and Torres Strait Islander Heritage Protection Act 1984* (Cth). The proposition of the *Hindmarsh Island Case* was that if the federal Parliament wished, it could enact racist laws, as the framers of the *Constitution* allowed 'the government to do and which Edmund Barton did with the creation of ghettos': at 9. This proposition 'is abhorrent to most Australians and is

with human rights progress made by other nations around the world, such as the UK and Canada.[56]

In summary, in the last century Australia's federal system has undergone a fundamental reshaping. State and Commonwealth Governments have found themselves, often against their desires, cooperating ever more closely on joint schemes of policy and administration.[57] As a consequence there has been a shift in the rules of the game of federal politics towards collaborative, as distinct from arm's-length, patterns of intergovernmental relations. While conflict and political disharmony remain commonplace, State and Commonwealth Ministers and officials have been more and more 'to be observed sitting around the table and devising joint schemes of policy and administration that emphasise national uniformity and the removal of interstate barriers and differences.'[58]

---

inconsistent with accepted community values, such as equity under the law': at 9. The *Hindmarsh Island Case* demonstrates, very clearly, that fundamental freedoms are often solely dependent on the 'wisdom and good sense of our legislators' and that this can easily be taken for granted: at 9.

[56] See also ALRC, Discussion Paper 80, above n46: at 22, 32; Richard Stone, *Civil Liberties and Human Rights* (Oxford University Press, 8th ed, 2010) [Stone examines the protection of human rights and liberties within the *British Constitution*]. The United Kingdom has recognised a cause of action for invasion of privacy in respect of misuse of private information, which some judges have described as a tort: *Campbell v MGN Ltd* [2004] 2 AC 457; see chapter 1, pp16-34 for a discussion of United Kingdom, Canadian and New Zealand human rights law.

[57] See Martin Painter, *Collaborative Federalism*, above n4. The *Council of Australian Governments* (COAG) and the *Special Premiers Conference* (SPC) was formed between 1990 and 1997: at 10-11. On January 1993 an agreement was reached under which the states would refer the power to the Commonwealth to apply uniform legislation for national competition policy, etc. It was agreed that the Council of the Federation would provide for a 'permanent, deliberative forum'. 'The States and Territories also agreed to the promotion of continuing reform and efforts to improve the structural efficiency of both the Australian Federation and the economy': at 42.

[58] See Martin Painter, *Collaborative Federalism*, above n4. Bob Hawke (Prime Minister – 1983-1991), 'New Federalism' in 1990 'was born out pragmatism rather than principle, by offering the states a platform on the new national stage': at 11. An important stimulus to the agenda of the 'new federalism was that overlap and duplication was futile': at 11. The delegates at the Constitutional Conventions 'failed to appreciate that simply naming powers was not tantamount to defining the ambit of those powers and

Nevertheless this process of cooperating collaborative change is evolutionary rather than revolutionary, and as such it is not a simple matter of a new set of rules, structures or habits of mind supplanting the old.[59] With the 2013 election of the federal Coalition Government, there is a chance that the process of collaborative federalism will be halted as other interests such as devolution, commercialisation and privatisation policies are advanced. The federal government's recent cooperative policy reversal is further highlighted by the abolition, in the 2014 federal *Budget*, of significant intergovernmental governing bodies such as COAG's monitoring body and the plan to cut funding and rationalise independent authorities, such as the OAIC.[60]

Despite the *Budget* not specifically targeting previous *EPR* and e-health government commitments, overall funding was drastically reduced and is to be revisited over the next two years by a proposed White Paper Report.[61] Media comments by the then federal Health Minister, Peter Dutton,[62] to the

---

that the world had changed and brought new roles and functions for government such as new technology': at 13. Bob Hawke's rhetoric in his 1990 speech (see Department of Prime Minister and Cabinet (DPMC) (1994), *Commonwealth-State Ministerial Councils: A Compendium*, 'focused repeatedly on 'the national interest' and sharing a commitment to a single national identity' ('one nation'): at 13; see also James Warden, "Federalism and the Design of the Australian Constitution" (1992) 27 *Australian Journal of Political Science* 143 [According to Warden, 'Yet within this splendid unity, we have imposed on ourselves a burden of different rules and regulations and requirements which needlessly weighs against the tremendous advantages we have as a nation-continent']: at 152. Hawke's call for intergovernmental cooperation and reduced 'fragmentation' supported 'a fundamentally centralist view of government cooperation and harmonisation': at 152. The central assumption was 'that uniformity and national standards were desirable national outcomes and that interstate coordination and other processes often lead to harmonisation': at 20-21.

[59] Martin Painter, *Collaborative Federalism*, above n4: at 153.

[60] See Federal *Budget 2014* published 13 May 2014; new federal *Budget* 2015 released (not included).

[61] See Ben Grubb, 'Abbott Government Uncomfortable with Freedom of Information Laws: Opposition' Sydney *Morning Herald* (Australia), 14 May 2014, 15; Andrew Bracey, 'Rich Should Cough Up: Dutton' *Medical Observer* (Australia) 28 February 2014, 18; see also Federal Health *Budget 2012-2013* for health services.

[62] Since 2015, the new federal Health Minister is Sussan Ley.

Australian Medical Association (AMA) and Australasian College of General Practitioners (ACGP) indicate that future e-health funding and the ongoing priority of *EPR* implementation (and by extension, healthcare privacy regimes) is not looking particularly favourable at this point in time.[63]

The merits and disadvantages of this ideological shift can only be guessed at, but a 'devolution' policy at this late stage will further complicate the unity of Australian health and privacy laws initiated by previous federal governments.[64] History assures us that state and territory governments will respond to this new development by combatively arguing about resource allocation. It is also likely that states and territories will embrace a more individual and idiosyncratic legislative approach in an already overly complex area.[65]

Consequently, 'the future contours of the federal system remain uncertain and contested.'[66] The new collaborative institutional forms and patterns may or may not take a lasting grip on Australian federal government, especially in light of Australian advocates of economic imperatives espousing free global market policies.[67]

---

[63] Andrew Bracey, 'Rich Should Cough Up', above n61: at 18.

[64] Martin Painter, 'The Persistence of Arm's-Length Federalism' in Martin Painter, *Collaborative Federalism*, above n4: at 187.

[65] See George Palmer and Stephanie Short, *Health Care and Public Policy* (Palgrave Macmillan, 4th ed, 2010) 10-11.

[66] Martin Painter, *Collaborative Federalism*, above n4: at 188.

[67] See, for example, Australian Coalition Government, *The Coalition's Policy on E-Government and Digital Economy* (September 2013); Australian Coalition Government, *The Coalition's Policy to Support Australia's Health System* (August 2013); Australian Government, *Budget* 2014-15 (13 May 2014).

Because of the constitutional framework, it is accurate to suggest that Australia does not have one national health system, but rather eight state and territorial health systems, intersecting with various Commonwealth policy and program objectives.[68] Thus, the legal mechanisms surrounding health (and healthcare privacy) systems 'represent a complex array of legislation, regulations and other legal instruments as well as health-related intergovernmental agreements.'[69] It is within this historical and complex (and increasingly global) picture, based upon reliance on 'fragmented' federalism, that modern privatised and commercialised healthcare and privacy rights are developing.[70]

In Australia privacy protection is primarily located in legislation rather than through common law development. The ALRC first considered the protection of privacy through tort law in 1979—*Unfair Publication: Defamation and Privacy*.[71] It also considered privacy in a later 1983 report, *Privacy:* ALRC 22, declining to recommend the creation of a general tort of invasion of privacy.[72] In a much later 2007 Discussion Paper 72, the ALRC proposed that a cause of action for 'a serious invasion of privacy

---

[68] See Palmer and Short, *Health Care and Public Policy*, above n65: at 17; see White, McDonald and Willmott, *Health Law in Australia,* above n50: at 16. See also the landmark case of *Secretary, Department of Health and Community Services (NT) v JWB* (1992) 175 CLR 218 ('Marion's Case'), [as to the relevance of human rights considerations to a decision about whether to sterilise an intellectually impaired minor].

[69] See White, McDonald and Willmott, *Health Law in Australia*, above n 50: at 73; Janine McIlwraith and Bill Madden, *Health Care and the Law* (Thomas Reuters, 6th ed, 2014); Bill Madden and Janine McIlwraith, *Australian Medical Liability* (LexisNexis, 2008); see also Sonia Allan and Meredith Blake, *The Patient and the Practitioner* (LexisNexis, 2014).

[70] See Victorian Law Reform Commission (VLRC), *Surveillance in Public Places*, Report No 18 (2010): at 149; NSWLRC, *The Offices of the Information and Privacy Commissioner*, Report No 125 (2009); Office of the Victorian Privacy Commissioner, to Senate Standing Committee on Legal and Constitutional Affairs on *Submission to Senate Standing Committee on Legal and Constitutional Affairs on Serious Invasions of Privacy in the Digital Era* (9 July 2012).

[71] ALRC, *Unfair Publication: Defamation and Privacy*: ALRC 11 (1979); see ALRC, *For Your Information: Australian Privacy Law and Practice*: Report 108 (May 2008): at 2537.

[72] ALRC, *Privacy:* ALRC 22 (1983): at 1081.

should be recognised by the legislature in Australia.'[73] However the main impetus for introducing Commonwealth privacy legislation was originally intended to implement Australia's obligations under the United Nations *International Covenant on Civil* and *Political Rights* (ICCPR) Article 17, as well as under the Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines).[74] Article 17 of the ICCPR states that:

> 1. No person shall be subjected to arbitrary or unlawful interferences with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.[75]

Further to ratifying the ICCPR on 13 August 1980, the Office of the United Nations (UN) High Commissioner for Human Rights in 1988 released General Comment Number 16. This paper discussed how 'the UN interprets art 17 and how it should be promoted through domestic law.'[76] As a result, all member State authorities are 'required to adopt legislation and other measures to give effect to the prohibition against such interferences and attacks as well as to protection of this right.'[77] The *Privacy Act 1988* (Cth) makes it clear that the legislation was intended to implement Australia's obligations relating to privacy under international obligations. The Act only concerned itself with public sector privacy and was restricted to information privacy, 'therefore [the Act] was not a full implementation in domestic law of the

---

[73] ALRC, Discussion Paper 72, above n46, Proposals 5-1 to 5-7.

[74] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); see also ALRC, Discussion Paper 72, above n46. ['The OECD Guidelines were developed to facilitate the harmonisation of national privacy legislation of OECD member countries, while upholding human rights, to prevent interruption in the international flow of personal information']: at 109.

[75] *International Covenant on Civil and Political Rights*, above n15.

[76] ALRC, Report 108, above n71: at 2539.

[77] ALRC, Report 108, above n71 quotes UN Office of the High Commissioner for Human Rights: at 2539.

meaning of art 17.'[78] In addition to the ICCPR and *Guidelines on the Protection of Privacy*, the Second Reading Speech to the Privacy Bill also referred to complying with the Council of Europe Convention for the *Protection of Individuals with Regard to Automatic Processing of Personal Data*.[79]

The *Privacy Act* represents 'the main federal privacy legislation regulating Australia's key information privacy law'.[80] The Act provides several paths for individuals where there has been a breach of the Australian Privacy Principles (APPs), as discussed later in the chapter. Other Commonwealth legislation such as the *Telecommunications Act 1997* (Cth) and *Telecommunication (Interception and Access) Act 1979* (Cth) also prohibits the disclosure of certain information by telecommunications providers.[81] Likewise, state and territory legislation creates information privacy requirements similar to those found under the *Privacy Act*.[82] However, as noted by the ALRC in 2013, this level of privacy protection may not be enough—*Serious Invasions of Privacy in the Digital Era: Discussion Paper 80*—stating that '[t]he challenge for lawmakers is how to ensure that law remains relevant, appropriate and workable in the light of technological advances.'[83] Additionally, ALRC—Discussion Paper 80—also reported that:

> The divergence in the recommendations of previous inquiries into privacy law, significant developments in other jurisdictions, concerns expressed in the community, continuing gaps in

[78] Ibid.

[79] ALRC, Report 108, above n71: at 4; see also *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981, Council of Europe, CETS No 108, (entered into force on 1 October 1985).

[80] ALRC, Discussion Paper 80, above n46. This proposal is discussed later in the chapter.

[81] Statutory protection such as *Broadcasting Services Act 1992* (Cth) and self-regulatory bodies (*Charter of Press Freedom* (2003)) through industry codes and guidelines may also help enforce privacy.

[82] ALRC, Discussion Paper 80, above n46: at 40-41.

[83] ALRC, Report 108, above n71: at 1.

> Australian common law and statute law protecting privacy, and new problems raised by the use of rapidly developing technologies … require detailed consideration by the ALRC …[84]

The following chapter analysis traces the evolution of Australian privacy law and practice by exploring common law healthcare privacy and confidentiality evolution, Commonwealth statutory privacy development, state/territory privacy regulations, as well as recent trends in *PCEHR* adoption and legislation. The legal discussion concludes by highlighting the ongoing significant role that law occupies in privacy protection in the modern digital information era.

III. COMMON LAW PRIVACY DEVELOPMENT IN AUSTRALIA

There is no common law right to privacy in Australia,[85] though the door has been opened for the development of such a right.[86] The lack of a common law right in this area can be traced back to the 1937 decision of the High Court in *Victoria Park Racing and Recreational Grounds Co Ltd v Taylor* ('*Victoria Park*'),[87] where it was held that a tort of breach of privacy should be rejected in Australian law. Australian courts applied this precedent for over 60 years and it was not until 2001 that the High Court, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ('*Lenah Game Meats*'),[88]

---

[84] Ibid 1-2; see also ALRC, *Serious Invasion of Privacy in the Digital Era:* Final Report 123 (3 September 2014).

[85] See ALRC, Discussion Paper 72, above n46: at 280-282; ALRC, Report 108, above n71: at 2539; ALRC, Discussion Paper 80, above n46: 49-50; chapter 1, pp26-34 [where it is also noted that in the past there has been no common law right to privacy in New Zealand, Canada and the United Kingdom]. However, in New Zealand, a tort of invasion of privacy has been recognised in *P v D* [2000] 2 NZLR 591: at 140 and *Hosking v Runting* [2004] NZCA 34: at 31-32, 140. In Canada 'a tort protecting privacy seems to be developing' — see *Motherwell v Motherwell* (1976) 73 DLR (3d) 62; *Burnett v The Queen in Right of Canada* (1979) 94 DLR (3rd) 281*; Ontario (Attorney-General) v Dieleman* (1994) 117 DLR (4th) 449; *Aubry v Duclos* (1996) 141 DLR (4th) 683.

[86] ALRC, Discussion Paper 72, above n46: at 280-281; ALRC, Discussion Paper 80, above n46: at 49; see also Department of the Prime Minister and Cabinet, Parliament of Australia, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (2011).

[87] (1937) 58 CLR 479; [1937] ALR 597.

[88] (2001) 208 CLR 199.

departed from its earlier decision. In obiter dicta, the High Court indicated that its previous decision in *Victoria Park*[89] did not stand in the path of the development of a cause of action for invasion of privacy.[90] Although they were provided with the opportunity to advance a cause of action for invasion of privacy in *Lenah Game Meats*, Gleeson CJ, along with Kirby J, nevertheless expressed caution about this 'new' tort, partly because of 'the lack of precision of the concept of privacy'[91] and suggested that:

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.[92]

After examining recent international developments on the tort of invasion of privacy[93] in *Lenah Game Meats*, Gummow and Hayne JJ (with whom Caudron J concurred), considered that privacy interests[94] are located in 'the fundamental value of personal autonomy' which could only be invoked by a natural person.[95] Accordingly, because the complainant was an artificial legal person (Lenah Game Meats Pty Ltd, a limited

---

[89] (1937) 58 CLR 479; see ALRC, Discussion Paper 72, above n47: at 281.

[90] (2001) 208 CLR 199 per Gummow and Hayne JJ, with whom Gaudron J concurred.

[91] (2001) 208 CLR 199 per Gleeson CJ: at 325-326.

[92] (2001) 208 CLR 199: at 325.

[93] See ALRC, Discussion Paper 72, above n46: at 282-283; ALRC, Report 108, above n 71: at 2540-2541. 'American Law Institute, *Restatement (Second) of Torts* (1977) §§ 625B-652E. Privacy torts have been well-established in the United States for many decades, although the protection they provide is limited by the constitutional protection of free speech in the First Amendment of the *United States Constitution*.' 'Some states such as California, have also introduced a statutory tort of invasion of privacy' (*California Civil Code* § 1708.8): at 2566. ALRC, Report 108, ibid 2543. In the United Kingdom, 'the tort of invasion of privacy is well developed': at 2543; discussed in chapter 1, pp26-34. 'The United Kingdom has developed extensive legal protection of privacy by extending the equitable action for breach of confidence (see *Campbell v MGN Ltd* [2004] 2 AC 457), under the influence of the *Human Rights Act 1998* (UK).' This Act requires 'the courts to give effect to the protection of rights and freedoms set out in arts 8 and 10 of the *European Convention on Human Rights*.' ALRC, Discussion Paper 80, above n46. The Canadian provinces 'of British Columbia, Manitoba, Newfoundland and Labrador, Quebec and Saskatchewan have enacted statutory torts for invasion of privacy': at 23.

[94] Such as reputation or commercial interests.

[95] (2001) 208 CLR 199, 256.

liability company), it was decided that the case was the wrong vehicle in which to explore the creation of a possible new tort based upon invasion of privacy.[96]

Since the High Court discussion in *Lenah Game Meats*,[97] the common law has remained under-developed. One of the classic problems with the development of law in a common law system is that it must await the arrival of a suitable dispute which raises the relevant issue. In the meantime, two lower Court decisions — *Grosse v Purvis*[98] and *Jane Doe v Australian Broadcasting Corporation*[99] — allowed common law recovery for breach of privacy. Despite these lower court decisions moving towards the recognition of the tort of invasion of privacy, 'no appellate court has confirmed the existence of this tort.'[100]

---

[96] (2001) 208 CLR 199, per Gummow, Hayne and Gaudron JJ: at 256-258.

[97] (2001) 208 CLR 199.

[98] [2003] QDC 151 [the Queensland District Court was required to consider the offence of the stalking of Alison Grosse (plaintiff) by Robert Purvis (defendant)]; see also ALRC, Discussion Paper 80, above n46: at 49-50.

[99] [2007] VCC 281 [this case concerned an ABC radio news broadcast that identified, by name and suburb, a female victim of rape in marriage, an offence under s4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic)].

[100] See ALRC, Discussion Paper 80, above n46: at 49-50; see also *John Fairfax Publications Pty Ltd v Hitchcock* [2007] NSWCA 364, where McColl JA noted that 'Australian common law does not recognise a tort of privacy': at 364; see *Giller v Procopets* [2004] VSC 113, 187-189 (Gillard J). In June 2013, the ALRC was given Terms of Reference for an inquiry into the protection of privacy in the digital era (ALRC, Discussion Paper 80 (2014)). The ALRC, New South Wales and Victorian Law Reform Commissioners have, at various times, recommended a statutory cause of action for serious invasions of privacy. See ALRC, Report 108, above n71; *NSWLRC*, *Invasion of Privacy*, Report No 120 (2009), where this was the major recommendation of the report; Victorian Law Reform Commission ('*VLRC*'), *Surveillance in Public Places:* Final Report No 18 (2010), Recommendations 22-24. The *VLRC* identified and recommended two causes of action, the first dealing with misuse of private information, which would be relevant to the health field. The contents of the recommendations are yet to be considered by government; also see George Williams, *Human Rights under the Australian Constitution*, above n38 [Williams identifies that common law in Australia affords 'bare protection of fundamental freedoms of the Australian people where they have not been abrogated by legislation']: at 16.

In *Grosse v Purvis,*[101] Skoien DCJ, drawing on the dicta of the High Court in *Lenah Game Meats,*[102] held that conduct which constituted the offence of stalking under s 359B of the *Queensland Criminal Code*[103] would also be actionable as a civil claim for invasion of privacy. Skoien DCJ adopted the view that a civil action for damages, based on the actionable right of an individual person to privacy, was a 'logical and desirable' step[104] and held that the defendant's action in stalking the plaintiff over a prolonged period of time constituted an actionable breach of privacy. His Honour, referring to *Lenah Game Meats,*[105] observed:

> The starting point of an analysis of the relevant elements of a possible tort of invasion of privacy is the decision of the High Court … The judgment is a very lengthy one which deals with a variety of issues … However in my view within the individual judgments certain critical propositions can be identified with sufficient clarity to found the existence of a common law cause of action for invasion of privacy.[106]

In *Jane Doe v Australian Broadcasting Corporation*,[107] the County Court of Victoria also accepted the emergence of a tort of invasion of privacy. Hampel J held that, in addition to breaching a statutory duty owed to the plaintiff by virtue of the *Judicial Proceedings Reports Act 1958* (Vic), the defendant broadcaster and employees were liable in equity for breach of confidentiality and in tort, for invasion of privacy for the 'unjustified publication of personal information.'[108]

---

[101] [2003] QDC 151.

[102] (2001) 208 CLR 199.

[103] *Criminal Code 1899* (Qld).

[104] *Grosse v Purvis* [2003] QDC 151, 442; see also ALRC, Discussion Paper 80, above n46: at 49.

[105] (2001) 208 CLR 199.

[106] [2003] QDC 151, 442.

[107] [2007] VCC 281.

[108] [2007] VCC 281; see also ALRC, Discussion Paper 80, above n46: at 49-50.

Since *Lenah Game Meats*,[109] a number of superior and lower courts have rejected privacy claims.[110] Commenting on *Grosse v Purvis*,[111] Heerey J in *Kalaba v Commonwealth* held that 'the weight of authority was against the proposition that the tort is recognised in common law.'[112] Similarly, in *Chan v Sellwood; Chan v Calvert*, Davies J described the position on the existence of the tort at common law as 'a little unclear'.[113] In *Gee v Burger*, McLaughlin J considered the matter 'arguable'.[114]

In *Giller v Procopets*[115] and in *Moore-Mcquillan v Work Cover Corporation*,[116] neither judgment considered *Grosse v Purvis*[117] in their deliberation and decisions. Katzmann J noted, in *Dye v Commonwealth Securities Ltd*, 'that it would be inappropriate to deny someone the opportunity to sue for breach of privacy on the basis of the current state of common law'.[118] In *Batistatos v Roads and Traffic Authority (NSW)*,[119] which did not involve issues directly related to privacy, Callinan J of the

---

[109] (2001) 208 CLR 199.

[110] See ALRC, Discussion Paper 80, above n46: at 49-50.

[111] [2003] QDC 151; see ALRC, Discussion Paper 80, ibid.

[112] [2004] FCA 763 (8 June 2004) 6.

[113] [2009] NSWSC 1335 (9 December 2009) 34.

[114] [2009] NSWSC 149 (13 March 2009) 53; see ALRC, Discussion Paper 80, above n46: at 50.

[115] (2008) 24 VR 1 [the defendant videotaped his sexual encounters with the plaintiff (his former wife) who was unaware of the filming. The defendant showed the videotapes to some people and distributed copies to others, including relatives and friends]. One of the causes of action pleaded by the plaintiff was a claim for invasion of privacy. The Supreme Court of Victoria rejected the claim, stating that 'the law has not yet developed to the point where the law in Australia recognises an action for breach of privacy'. See also ALRC, Discussion Paper 80, above n46: at 49-50.

[116] [2007] SASC 55 [the Supreme Court of South Australia considered the appellant's claim for breach of privacy, which was kept under video surveillance by a private investigator engaged by WorkCover]. In this case, the Court accepted the current law, as stated in *Lenah Game Meats* (2001) 208 CLR 199, that 'there is no common law right to privacy in Australia.' See also ALRC, Discussion Paper 80, above n46: at 49-50.

[117] [2003] QDC 151.

[118] [2010] FCA 720, 290. However Katzmann J refused leave to the plaintiff to amend her pleadings to include such a claim citing various grounds. See also ALRC, Discussion Paper 80, above n46: at 49-50.

[119] [2006] HCA 27.

High Court, in obiter dicta, reiterated his statement in *Lenah Game Meats* that 'the time was ripe for consideration by the law of a cause of action for invasion of privacy.'[120]

Basten J in *Maynes v Casey*, referring to *Lenah Game Meats*[121] and *Giller v Procopets*,[122] stated that 'these cases may well lay the basis for development of liability for unjustified intrusion on personal privacy'.[123] In *Saad v Chubb Security Australia Pty Ltd*, Hall J refused to strike out a claim for breach of confidence holding that a 'cause of action for breach of confidence based on invasion of the plaintiff's privacy would be futile or bad law'.[124]

Additionally, in *Sands v State of South Australia*, Kelly J said that 'the ratio decidendi of the decision in Lenah is that it would require a further development in the law to acknowledge the existence of a tort of privacy.'[125] Further, in the recent case of *Doe v Yahoo! 7 Pty Ltd*, Smith DCJ stated 'it seems to me there is an arguable case of invasion of privacy…I would be very hesitant to strike out a cause of action where the law is developing and is unclear.'[126]

A *Causes of Action at Common Law*

Despite the 'door' being left open for a tort of privacy, there are a number of existing causes of action at common law[127] which may, in some cases, be evoked in order to

---

[120] [2006] HCA 27 cites the decisions in *Douglas v Hello! Ltd* [2001] QB 967; [2003] 1 All ER 1087; [2006] QB 125: at 216; see also *HRH Prince of Wales v Association of Newspapers Ltd* [2006] EWHC 522 (Ch).

[121] (2001) 208 CLR 199.

[122] (2008) 24 VR 1; see ALRC, Discussion Paper 80, above n46: at 50.

[123] [2011] NSWCA 156 (14 June 2011) Allsop P agreed with Basten J: at 35.

[124] [2012] NSWSC 1183, 1183.

[125] [2013] SASC 44 (5 April 2013) 614; see ALRC, Discussion Paper 80, above n46: at 50.

[126] [2013] QDC 181 (9 August 2013), 310-311; see ALRC, Discussion Paper 80, ibid.

[127] See Harold Luntz and David Hambly, *Torts: Cases and Commentary* (LexisNexis, 7th ed, 2011). The characteristics that distinguished trespass from the action on the case were, firstly, that the interference

indirectly protect personal privacy.[128] These actions include: the tort actions for trespass to the person,[129] trespass to land[130] and the tort of nuisance;[131] the tort of defamation,[132] and an equitable action for breach of confidence.[133] For instance, the tort of trespass to land is capable of providing direct protection against invasions of privacy by those who enter private property, without consent, to install surveillance

---

with the plaintiff's person, land or goods must be direct. It must be part of the defendant's act and not merely a consequence of it. It is from the action on the case that torts such as negligence and nuisance are derived: at 627-628. The tort of trespass to the person consists of battery and assault, and false imprisonment. The tort of battery is committed by directly and intentionally bringing about harmful or offensive contact with the person of another. In *Mallette v Shulman* (1991) 2 Med LR 162 (CA Ontario), [the plaintiff was given a blood transfusion after a serious car accident this was held to be a battery]; *Fontin v Katapodis* (1962) 108 CLR 177; [1962] HCA 63 [where K sued F, a hardware shop assistant, in battery]. K had purchased goods at the shop and later returned them. F accused him of failing to pay for the goods). The tort of assault is committed by intentionally creating in another an apprehension of imminent harmful or offensive contact. False imprisonment is committed by directly and intentionally confining the plaintiff within an area fixed by the defendant, without legal authority (see, for example, *Bird v Jones* (1845) 7 QB 742; 15 ER 668 Court of Queen's Bench).

[128] See ALRC, Discussion Paper 80, above n46: at 20, 43.

[129] Luntz and Hambly, *Torts: Cases and Commentary*, above n127 [the essential elements of trespass to person such as Assault and Battery and false imprisonment are outlined]: at 649-662.

[130] Ibid [the tort of trespass to land lies only where there is a 'direct' invasion of land in possession of the plaintiff. Trespass to land is committed by 'directly and intentionally (or, it would seem, negligently) entering or remaining upon, or causing some object to come into contact with, land in the possession of another, without consent of the person in possession or other legal justification or excuse']: at 680.

[131] Ibid [whereby the tort of trespass to land lies only in a 'direct' invasion of land, an 'indirect' interference with the possessor's use and enjoyment of land is in nuisance]: at 731; Private nuisance — see, for example, *Halsey v Esso Petroleum Co Ltd* [1961] 2 All ER; [1961] 1 WLR 683 Queen's Bench Division [where the plaintiff complained of activities relating to the defendants' nearby oil depot].

[132] See Des Butler and Sharon Rodrick, *Australian Media Law* (Thomas Reuters, 4th ed, 2011). Defamation occurs where one person communicates, by word, photographs, video, illustrations or other means, material which has the effect or tendency of damaging the reputation of another; see, for example, *Gorton v Australian Broadcasting Commissioner* (1973) 22 FLR 181, 25 [where the then Prime Minister sued in an Australian Capital Territory court on the basis of matter broadcast simultaneously in New South Wales, Victoria and the Australian Capital Territory]. See also McIlwraith and Madden, *Health Care and the Law*, above n69: at 328; *Rogers v Nationwide News Pty Ltd* (2003) 216 CLR 327 [This case involved the newspaper publication of an article claiming that Mrs Whitaker, the plaintiff in *Roger v Whitaker* (1992) 175 CLR 479 (*Rogers Case*) had been 'blinded by a surgeon's negligence' defamed Dr Rogers, the defendant surgeon. The 1992 High Court *Rogers Case* concerned medical negligence, resulting in damages being awarded to the Plaintiff (Mrs Whitaker). However, following the *Rogers Case*, a separate court action between Mrs Whitaker and the Australian Taxation Office (ATO) was commenced]. This later tax case resulted in the defamatory newspaper article and subsequent defamation action by Dr Rogers against the publishers (*Rogers V Nationwide New Pty Ltd* (2003) 216 CLR 327).

[133] See McIlwraith and Madden, 'Patient Privacy and the Duty of Confidentiality' in McIlwraith and Madden, *Health Care & the Law*, above n69: at 311, 312.

equipment,[134] photograph, film, and record or interview the occupants of the land.[135] The modern action for trespass to land 'will provide a remedy for invasion of privacy only incidentally when it happens to be otherwise available.'[136] Alongside trespass to property protection rights, there is also the tort of trespass to the person which includes assault, battery and false imprisonment actions.[137] Significantly, 'the common law maintains that any unwanted interference with a person's body or the creation of fear of such interference is an actionable wrong.'[138] According to the law of trespass to person no such action (touching) 'may be taken without the person's consent', other than in limited situations.[139] This right afforded by the law to obtain an individual's consent may provide an 'indirect' way of protecting bodily privacy rights.

Private nuisance, on the other hand, offers limited protection against breaches of privacy. It does not provide protection against casual observation, filming or recording outside the property. Private nuisance may be used in a situation where

---

[134] See *Bernstein v Skyviews & General Ltd* [1978] QB 479; [1977] 2 All ER 902 [The defendant's took a single aerial photograph of Lord Bernstein's country house in Kent]; see *Bathurst CC v Saban* (1982) 2 NSWLR 704 ['Peep through my window from afar and I may be remediless; put a foot over my boundary while you look and the invasion of my dignity can be taken into account in damages awarded for your trespass']: at 708; see also Luntz and Hambly, above n127. 'On a limited scope of the law of torts for protecting privacy': at 74.

[135] See *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457, 456 (Young J) [The plaintiff sought an injunction to restrain the defendant from televising a videotape allegedly made in the course of a trespass on the plaintiff's property]; *Emcorp Pty Ltd v Australian Broadcasting Corporation* [1988] 2 Qd R 169, 176 (Williams J) [arose out of a visit by a television crew, which filmed an interrogation of the plaintiff's staff by a reporter who alleged that the plaintiff had committed a criminal offence].

[136] Luntz and Hambly, *Torts: Cases and Commentary*, above n127: at 74.

[137] Ibid [Trespass to Person]: at 627.

[138] McIlwraith and Madden, *Health Care & the Law,* above n69: at 71.

[139] Ibid; exceptions to obtaining consent would include situations where there is an emergency: at 79-80.

the plaintiff is seeking to protect some private interest, such as indirect interference with the possessor's use and enjoyment of land.[140]

Defamation action,[141] and other innominate torts in certain situations, may incidentally provide a remedy for breach of privacy.[142] According to Luntz, 'the dignitary interest in one's person and the interest in privacy may also be incidentally protected by the tort of defamation, but primarily the remedy is there to protect the interest in reputation.'[143] However, since 1 January 2006 the defence of justification in New South Wales has been changed so that truth alone constitutes a defence under the *Defamation Act*.[144] New provisions were adopted as part of uniform defamation legislation among the states and territories.[145] This change makes defamation less effective in providing privacy protection to health-related information.[146]

---

[140] *Raciti v Hughes* (1995) 7 BPR 14 [the court, in this case, granted the plaintiffs' application for an injunction against an adjoining occupant to prevent the operation of video surveillance equipment, which overlooked their backyard]. The defendant was monitoring every activity of neighbours, including the use of bright light was held to amount to nuisance. Some courts have used private nuisance to deal with telephone harassment, considering it as invasive of a person's privacy.

[141] See generally Butler and Rodrick, *Media Law in Australia*, above n132: at 25.

[142] In *Ettinghausen v Australian Consolidated Press Limited* (unreported, NSWCA, 13 October 1993) [a photograph was taken of a well-known sports person in the shower and published in a magazine]. The New South Wales Supreme Court held that publication of the photograph defamed him. Traditionally, s15 of the *Defamation Act 1974* (NSW) required that the defendant show that the imputation was not only substantially true, but also that it relates to a matter of 'public interest'. This requirement ('public interest' and 'public benefit') was described as 'the closest the law of defamation comes, as presently framed, to protect privacy, at least in those jurisdictions which so limit the defence of truth': see *Johnston v Australian Broadcasting Commission* (1993) FLR 307, 312 (Higgins J).

[143] Luntz and Hambly, *Torts: Cases and Commentaries*, above n127: at 75; see also ALRC, *Unfair Publication: Defamation and Privacy:* ALRC 11 (1979).

[144] See, for example, *Defamation Act 2005* (NSW) s25.

[145] See *Civil Law (Wrongs) Act 2002* (ACT) s 135; *Defamation Act 2006* (NT) s 22; *Defamation Act 2005* (Qld) s25; *Defamation Act 2005* (SA) s 23; *Defamation Act 2005* (Tas) s 25; *Defamation Act 2005* (WA) s25; *Defamation Act 2005* (Vic) s25.

[146] Bruce Clarke, Brendan Sweeney and Mark Bender, *Marketing and the Law* (LexisNexis, 4th ed, 2011). Another possible tort relating to privacy is 'passing off'. This tort involves the appropriation of the name, image or likeness of a person without his or her consent: at 173. This is arguably a form of invasion of privacy to the extent that his or her interest in the exclusive use of his or her own identity is infringed. However, this tort is limited to commercial situations and is of limited value to healthcare

The innominate tort of intentional infliction of nervous shock and psychiatric illness was discussed in the English case of *Wilkinson v Downton*[147] and the Australian case, *Mount Isa Mines Ltd v Pusey*.[148] However, many invasions of privacy will not result in psychiatric damage and unless it is extended to mental *distress*, *Wilkinson v Downton*[149] may prove of limited value in the context of privacy protection.[150]

B *Breach of Confidence*

In a search for a robust theory of privacy it is essential to explore the role of confidentiality. Although confidentiality and privacy are often seen as interchangeable, they have developed somewhat independently and are different concepts. Confidentiality is concerned with security of information. The concept is linked 'to personal dignity and patient autonomy and is an equitable and legal concept

privacy. In *Henderson v Radio Corporation Pty Ltd (*1960) 60 SR NSW 576, the plaintiff succeeded in obtaining an injunction to restrain the defendant from releasing a record of ballroom dancing music, which displayed the plaintiff's photograph on the cover without consent.

[147] [1897] 2 QB 57; see also *Coultas v Victorian Railways Commissioners* (1886) 12 VLR 895 [Mary Coutas was being driven in a buggy by her husband, her husband drove through a railway crossing as a train was approaching, she suffered a miscarriage as a result of the shock]; for tort development, see also *Janvier v Sweeney* [1919] 2 KB 316; *Carrier v Bonham* [2001] QCA 234; *Giller v Procopets* [2008] VSCA 236 [The husband videotaped himself with Ms G having sexual intercourse on at least 10 occasion without her knowledge]; *Jaensch v Coffey* (1984) 155 CLR 549; 54 ALR 417 [The plaintiff developed severe anxiety and depression after it was revealed to her that her husband had been severely injured in a collision]. Two aspects of the rule in *Wilkinson v Downton* [1897] 2 QB 57 potentially limit its application to cases involving invasion of privacy. The first aspect relates to its uncertain scope and the second aspect requires that the plaintiff must show that his or her reaction to the defendant's conduct is accompanied by some 'physical injury'. Consequently, mere distress will not suffice.

[148] (1970) 125 CLR 383; [1971] ALR 253 [the plaintiff was working with two electricians who were horribly burnt at work and as a result, the plaintiff suffered a schizophrenic episode]. In *Wilkinson v Downton* [1897] 2 QB 57 [the defendant, by way of a practical joke, told the plaintiff that her husband had met with an accident and was seriously injured]. 'As a result, the plaintiff suffered a violent nervous shock with serious physical consequences, which the defendant was held liable for.' The basis of the decision is that 'If a person deliberately does an act of a kind calculated to cause physical injury for which there is no lawful justification or excuse and in fact causes injury to that other person he is liable in damages'.

[149] *Wilkinson v Downton* [1897] 2 QB 57.

[150] *Wainwright v Home Office* [2004] 2 AC 406 [involved the strip search of a mother and son for drugs on a prison visit].

long recognised in the law, whereas privacy is a more modern notion, primarily based on information protection.'[151] Characteristically, 'the duty to maintain confidence is also expressed through various authorities, including professional codes and charters,[152] international obligations[153] and common law precedents.'[154]

The duty to preserve confidence in healthcare arises because of 'the specific relationship between the professional and the patient and only to information that is confidential in nature.'[155] Confidential information is information that is not generally or publically known, but is known to a restricted number of individuals.[156] Similarly,

---

[151] See White, McDonald and Willmott, *Health Law in Australia*, above n50: at 301; see also Graeme Laurie, *Genetic Privacy* (Cambridge University Press, 2002) 212; *A-G v Guardian Newspaper (No 2)* [1990] 1 AC 109 (the *Spycatcher Case*) [where Lord Goff summarised the law regarding confidential information]; *Seager v Copydex* [1967] 1 WLR 923 per Lord Denning established the principle that 'a person who received information in confidence shall not take unfair advantage of it … the person must not make use of it to the prejudice of the person who gave it without obtaining consent': at 658; see *Furniss v Fitchet* [1958] NZLR 396 [a husband and wife were having marital difficulties and attended the same doctor who wrote a report about Mrs Furniss]; *Tame v New South Wales* (2002) 211 CLR 317 [these two cases were dealt with by the HC and were about a psychiatric illness as a reaction to an erroneous statement by a police officer in a traffic accident report].

[152] See Australian Medical Association (AMA), Code of Ethics (2006), 1.1 (12) under 'Patient Care', 1.1 (13) is also relevant to the duty — 'Upon request by your patient make available to another doctor a report of your findings and treatment'; see also *Health Care Complaints Commission v Khan* [2008] NSWNMT 15 [where an enrolled nurse was prosecuted by the Health Care Complaints Commission for inappropriate disclosure of patient personal information]; see generally, Nurses Registration Board of New South Wales, *Professional Conduct* (New South Wales Registration Board, 2001).

[153] See Declaration of Geneva, Editorial Revision, 2006. 173th Council Session of the World Medical Organisation, Divonne-les-Bains; European Convention of Human Rights and Fundamental Freedoms (1950) (European Convention) as amended by Protocol 11 (1998) and Protocol No 14 (2010) opened for signature 13 May 2004, Council of Europe Treaty Series No 194 (entered into force 1 June 2010), European Convention of Human Rights, *International Code of Medical Ethics Declaration of Geneva* (1950); *Z v Finland* (1997) 25 EHRR 371 (ECtHR); see, for example, *MS v Sweden* (1997) 45 BMLR 133 (ECtHR).

[154] See *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Service*s *& Health* (1990) 22 FCR 73 at 121 (Gummow J recognised that equity acts can protect confidential information); *Furniss v Fitchett* [1958] NZLR 396; *Duncan v Medical Practitioners Disciplinary Committee* [1986] 1 NZLR 513; *Breen v Williams* (1996) 186 CLR 71; Moira Paterson, *Freedom of Information and Privacy in Australia* (LexisNexis, 2005): at 17; L McRae, "Withholding Medical Records without Explanation: A Foucauldian Reading of Public Interest" (2009) 17(3) *Medical Law Review* 438.

[155] Allan and Blake, *The Patient and the Practitioner*, above n69: at 300.

[156] See *A-G v Guardian Newspapers (No 2)* [1990] 1 AC 109; see also Kim Forrester and Debra Griffiths, *Essentials of Law for Health Professionals* (Elsevier Australia, 2009); McIlwraith and Madden, *Health Care and the Law*, above n69: at 311; see also Danuta Mendelson, "The Duchess of Kingston's Case, the Ruling of Lord Mansfield and Duty of Medical Confidentiality in Court" (2012) 35 *International Journal of Law*

once information moves from the private sphere to the public sphere, it loses the necessary quality of confidence. Thus 'trade secrets, business practices and government data, as well as personal information can be confidential.'[157] As a result of extensions (such as contracts) in the law, the equitable action for breach of confidence is a powerful legal weapon to protect individuals from the unauthorised disclosure of confidential information.[158] 'There does not have to be a contract between people for there to be an obligation to maintain the confidentiality of information.'[159]

The issue of the future development of an action for a breach of confidence to protect a person's privacy was foreshadowed by Gleeson CJ in *ABC v Lenah Games Meat*, as a venue that could be further developed by courts.[160] Gleeson CJ stated that 'an equitable action for breach of confidence may be the most suitable legal action for protecting people's private information from disclosure', noting that '[t]he law should

---

and Psychiatry 480: at 480-489. However, there are a number of common law immunities, including Public Interest Immunity under s 130 of the *Uniform Evidence Act 2008* (Cth) and at common law, under the principle espoused in *Sankey v Whitlam* (1978) 142 CLR 1 per Gibbs ACJ: at 38. The scope of the public interest in confidentiality of health records was also discussed in *Royal Women's Hospital v Medical Practitioners Board of Victoria* (2006) 15 VR 22, which was an appeal from *Royal Women's Hospital v Medical Practitioners Board* [2005] VSC 225 (affirmed) [the case involved termination of a suicidal mother's pregnancy at 32 weeks, after ultrasound tests indicated that the foetus had skeletal dysplasia]. Although the Medical Practitioner's Board was empowered to investigate the matter, the Royal Women's Hospital resisted production of the mother's medical records. The hospital argued, inter alia, public interest immunity from disclosure of medical records.

[157] Graeme Laurie, *Genetic Privacy*: *A Challenge to Medico-Legal Norms* (Cambridge University Press, 2002) 213.

[158] See McIlwraith and Madden, *Health Care and the Law*, above n69: at 318.

[159] An action for breach of confidence can be brought where: the information is confidential in nature; it has been imparted in circumstances giving rise to an obligation of confidence; and it is used without authority to the detriment of the person who gave it; see *Argyll v Argyll* [1965] 1 All ER 611 [where the Duke of Argyll sought to sell information about the private life of his estranged wife, the Duchess of Argyll, to a newspaper]; *Giller v Procepets* [2008] VSCA 236 [where Mr P videotaped himself and Mrs G having sexual intercourse on at least 10 separate occasions, without her knowledge].

[160] See ALRC, Discussion Paper 80, above n46: at 180.

be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy.'[161] Further stating that:

> [E]quity may impose obligations of confidentiality even though there is no imparting of information in circumstances of trust and confidence. And the principle of good faith upon which equity acts to protect information imparted in confidence may also be invoked to restrain the publication of confidential information improperly or surreptitiously obtained … For reasons already given, I regard the law of breach of confidence as providing a remedy, in a case such as the present, if the nature of the information obtained by the trespasser is such as to permit the information to be regarded as confidential.[162]

Generally, in Australia the traditional claims for breach of confidence will rely upon a number of established legal remedies including: 'injunctions for the anticipated or continuing breach of confidence; compensation for economic loss due to the breach or an account of anticipated profits arising from the breach.'[163] These remedies are usually about confidence relating to commercial, government or personal information. However, in *Serious Invasions of Privacy in the Digital Era*: Discussion Paper 80, the ALRC highlighted a number of limitations that existed in the present law. Noting that where the breach of confidence in relation 'to personal information or private information has occurred and an injunction is futile, the consequence that a claimant is most likely to suffer is emotional distress,' rather 'than harm in the way of economic loss.'[164] This proposition was supported by Tilbury who acknowledged that 'the very object of the action [for invasion of privacy] will be to

---

[161] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 per Gleeson CJ: at 40.

[162] ALRC, Discussion Paper 80, above n46: at 180; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 per Gleeson CJ: at 34, 39, 40, 55.

[163] ALRC, Discussion Paper 80, above n46: at 182.

[164] Ibid.

protect against [mental or emotional distress], at least in part.'[165] While the limited circumstances for the recovery of compensation 'for 'mere' emotional distress has been a 'perennial issue for the law torts'',[166] the issue of 'recovery in equity has not been raised in Australia until the case of *Giller v Procopets*.'[167]

As discussed, the tort actions of trespass to land, trespass to person, nuisance and breach of confidentiality do not provide protection from unauthorised and serious intrusions into a person's private activities in numerous situations, so they are of limited value in relation to invasion of privacy protection.[168] In addition, based on these tort actions,[169] tort does not provide a remedy for the intentional infliction of emotional distress which does not amount to psychiatric illness.[170] While the equitable action for breach of confidence can provide effective legal protection to prevent the disclosure of private information, it is currently less effective after a wrongful disclosure, because it is unclear whether a plaintiff may recover compensation for emotional distress.[171] There is continuing uncertainty as to the

---

[165] ALRC, Discussion Paper 80, per Michael Tilbury, 'Coherence, Non-Pecuniary Loss and the Construction of Privacy' in Jeffrey Berryman and Rick Bigwood (eds), *The Law of Remedies: New Directions in the Common Law* (Irwin Law, 2010) 127 cited by ALRC, Discussion Paper 80, above n46: at 182.

[166] Ibid; see *Giller v Procopets* (2008) 24 VR 1 (Neave JA and Ashley JA, Maxwell P dissenting); see Barbara Mc Donald, 'Tort's Role in Protecting Privacy: Current and Future Directions' in James Edelman, James Goudkamp and Degeling (eds), *Torts in Commercial Law* (Thomas Reuters, 2011).

[167] ALRC, ibid; *Giller v Procopets* (2008) 24 VR 1.

[168] Trespass to person requires bodily contact, or a threat of such contact, to be actionable. Both trespass to land and nuisance protect only the occupier of the relevant land, and the former requires an intrusion onto the land.

[169] Trespass, nuisance and defamation.

[170] *Wainwright v Home Office* [2004] 2 AC 406*; Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417

[171] See *Giller v Procopets* (2008) 24 VR 1; *Wilkinson v Downton* (1897) 2 QB 57; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 71; see ALRC, Discussion Paper 80, above n47. *Lord Cairns' Act* (21 & 22 Vict c27) 1858, where a court has power to grant an injunction or to order specific performance, the court may award damages to the party injured: at 183; *Supreme Court Act 1970* (NSW), s68.

relevant principles to be applied when a court is considering whether to grant an interlocutory injunction to restrain the publication of true, private information.[172] Unless the area is developed by the courts the present situation creates a 'gap' and a measure of 'uncertainty' in the law.[173]

This legal 'uncertainty' in personal privacy protection is especially pertinent in the digital information era given the current federal Coalition Government's reluctance to clarify the situation by adopting statutory protection. It was recommended by the ALRC and other state independent bodies,[174] that the Commonwealth Government consider enacting a statutory cause of action and that this be contained in a new, stand-alone, invasion of privacy Act, the general consensus being that the likely direction of the future development of the common law is uncertain.[175] It is also acknowledged that although the breach of confidence is well supported by the law, realistically pursuing litigation in equity and tort courts is an

---

[172] ALRC, Discussion Paper 80; above n47; see also George Williams, *Human Rights under the Australian Constitution*, above n28 [provides an analysis of the gaps between the constitutions of the Australian states and the self-government Acts of the territories, for example, *Northern Territory (Self-Government) Act 1978* (Cth) s50 and the *Australian Capital Territory (Self-Government) Act 1988* (Cth) s23 – provide that the respective parliaments cannot legislate for the 'acquisition of property otherwise than on just terms'. This mirrors the limitation on Commonwealth power found in s51 (xxxi) of the Australian Constitution. None of the state constitutions contains a like provision]: at 8

[173] ALRC, Discussion Paper 80, above n46: at 47-49. The ALRC, 'recognises a number of significant 'gaps' or uncertainties in existing privacy protection.' For example, 'further uncertainty, or at least some debate, as to the relevant principles to be applied when a court considers whether to grant an interlocutory injunction' to restrain certain behaviour: at 47.

[174] See NSWLRC, *Invasion of Privacy*: Report 120 (2009); Victorian Law Reform Commission, *Surveillance in Public Places*: Report 18 (2010).

[175] ALRC, Discussion Paper 80, above n47: at 20, 50; see also, from the chapter discussion, that invasion of privacy has been recognised by two lower court decisions: *Grosse v Purvis* [2003] QDC 151 and *Jane Doe v Australian Broadcasting Board* [2007] VCC 281. Both cases were settled before the appeals, by the respective defendants, were heard.

expensive, time consuming and complicated option, which is likely beyond the general reach of most ordinary citizens.[176]

Consequently, the general consensus is that the future development of the tort of invasion of privacy is uncertain and remains in legal 'limbo'.[177] However, what can be determined from the case law is that an expanded judicial view of modern-day privacy protection is not a forthcoming option in Australia unless Parliament says so. The judiciary in Australia is still impeded by the narrow interpretation of privacy concepts and strict Parliamentary sovereignty rules. As a consequence, 'it is fair to say that this area has not significantly progressed since *Lenah Game Meats* in 2001.'[178]

It can be observed 'that the concern in protecting and keeping a person's health records private and confidential is one shared by the whole patient community.'[179] This apprehension emanates from the fact that a person's health information might affect a person's treatment in the employment or insurance context, as well as a widely held belief that healthcare information is essentially 'private' in nature.[180] Moreover it can also be illustrated that international and Australian citizen frustration relating to adequate individual privacy protection in the digital economy represents a serious problem that needs to be adequately addressed by law. This is evidenced by recent worldwide publicity supported by influential local (and international) members of society, calling for the United Nations to urgently intervene by declaring a *Bill of*

---

[176] See Hilary Astor and Christine Chinkin, *Dispute Resolution in Australia* (LexisNexis, 2nd ed, 2002).

[177] ALRC, Discussion Paper 80, above n46: at 193.

[178] (2001) 208 CLR 199.

[179] ALRC, Discussion Paper 80, above n46: at 319.

[180] ALRC, *Essentially Yours: The Protection of Human Genetic Information in Australia*: Report 96 (2003) for discussion of the basis of patients' concerns about disclosure of their health information: at 3.37-3.39.

Digital Rights to Protect Privacy to ensure citizen rights; this demonstrates the political and social reach of the privacy protection problem.[181]

To conclude, it has been the introduction of legislation, rather than judge-made changes, which has sought to address 'gaps' in coverage.[182] As noted by Allan:

> [T]hese changes have created questions about the relationship of the common law protections to the statutory regime, particularly those associated with the exceptions that permit access to information under the privacy legislation and which appear to conflict with the duties of confidentiality. The problem is complicated by the fact that much of the relevant legislation preserves the common law duties as they exist.[183]

If the 'coverage' issue remains 'unaddressed' it will continue to be a source of confusion for custodians of health information.[184]

IV. COMMONWEALTH PRIVACY STATUTORY PROTECTION

As mentioned earlier, the *Privacy Act 1988* (Cth) represents the main federal privacy legislation regulating the handling of personal information and outlines certain safeguards that government, private sector organisations and individuals must observe when collecting, storing, using and disclosing personal information, including health information. The *Privacy Act* purports to 'make provision to protect

---

[181] See Bridie Jabour, 'Australian Authors Join Call for UN Bill of Digital Rights to Protect Privacy' *The Guardian* (United Kingdom), 10 December 2013, 1. The petition to the United Nations states that mass surveillance treats everyone like a suspect, overturning the presumption of innocence and making the individual 'transparent', while the state operates in secret. "A person under scrutiny is no longer free; a society under surveillance is no longer a democracy": at 2.

[182] See *Breen v Williams* (1995) 186 CLR 71 per Gaudron and McHugh JJ. [Highlighted a number of 'gaps' in the way in which common law deals with healthcare information]: at 107.

[183] Allan and Blake, *The Patient and the Practitioner*, above n69: at 318; see, for example, *Information Act 2002* (NT) s55; *Right to Information Act 2009* (Tas) s39; *Freedom of Information Act 1989* (ACT); *Freedom of Information Act 1982* (Vic) s35.

[184] Allan and Blake, *The Patient & the Practitioner*, above n69: at 318.

privacy of an individual, and for related purposes.' [185] The Act is generally the principal mechanism for protecting public and private sector privacy in Australia.

The objective of the *Privacy Act* is to balance the protection of the privacy of individuals with the interests of public and private sector entities, in carrying out their lawful and legitimate functions and activities. It enables the personal information of an individual to be collected, used and disclosed in certain circumstances,[186] and recognises that collection, use, storage and sharing of personal information, including its release without an individual's knowledge or consent, can amount to interference with privacy.[187] In addition, the Act details the conditions where this type of interference with individual privacy is authorised by law.[188]

However, section 3 of the *Privacy Act* makes it clear that the Australia Parliament did not intend to 'cover the field' and override state and territory laws relating to the protection of personal privacy and states:

> It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information … and is capable of operating concurrently with this Act.

---

[185] Allan, et al, *The Patient & the Practitioner*, above n69: at 318.

[186] See, for example, *APP* 3 and *APP* 6.

[187] See Australian Parliament, House of Representatives, *Explanatory Memorandum*, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 2012.

[188] Ibid. This authorisation is based upon legitimate objectives such as 'imminent threat to life' and must be 'reasonable, necessary and proportionate': at 15-17. Such activities include the promotion of the government's service delivery, taxation, law enforcement and national security objectives, and the needs of business to offer services to the public. The overall context of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) takes into account the changing advances in technology, modern electronic healthcare systems and aims towards flexibility of the system.

Other limitations to the scope and operation of the *Privacy Act* are found in s 16E, which specifically excludes personal, family or household affairs from the operation of the Act:

> Nothing in the National Privacy Principles applies to: (a) collection, holding, use, disclosure or transfer of personal information by an individual; or (b) personal information held by an individual; only for purposes of, or in connection with, his or her personal, family or household affairs.

The Act itself provides a range of definitions of terms used in the legislation such as 'sensitive information' and 'health provider'.[189] It includes Privacy Codes that clarify codes of conduct and public interest determinations. It also sets out the functions of the Information Commissioner, including his or her role in complaint handling.[190] The Act applies to acts done and practices engaged in by agencies or organisations[191] and contain a range of exemptions and exceptions.[192] An 'exemption' applies where a specified entity or class of entity is not required to comply with the privacy principle (e.g. small business exemption), whereas an 'exception' applies where a requirement

---

[189] *Privacy Act 1988* (Cth) s 6(1) defines 'sensitive information' to 'mean (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; but is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is otherwise health information.'

[190] The overall structure of the *Privacy Act* is set out as follows — the definition and interpretation of terms are set out in Part II. Part III deals with information privacy such as interference with privacy (s 13) and interference with privacy by organisations (s 14). Part IIIA requires reporting of privacy breaches and contains the Privacy Codes. The function of the Information Commissioner is set out in Part IV and privacy investigations are located in Part V. Part VI deals with public interest determinations. The obligation of confidence is found in Part VIII. Part IX outlines miscellaneous events, such as the guidelines about genetic information (s 95AA) and Regulations (s 100).

[191] *Privacy Act* s6(1), which defines 'organisations' as an individual, a body corporate, a partnership and any other unincorporated association or a trust, but specifically excludes many private sector small business operators and registered political parties'.

[192] *Privacy Act* sets out exemptions and exceptions.

in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct.[193]

Over the years the *Privacy Act* has been amended by a raft of amending legislation. For instance in December 2000, the *Privacy Amendment (Private Sector) Act 2000* (Cth) was enacted by federal Parliament, extending coverage of the Act to most private sector organisations. At the time, the amendments included the National Privacy Principles (NPPs), which provided the benchmark for industry codes.[194]

Subsequently, the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) amended the *Privacy Act* by introducing a 'unified' set of privacy principles, the Australian Privacy Principles (*APPs*)[195] that now supersede the previous IPPs and NPPs and cover both public and private sector information obligations.[196] The fact that there is now a single set of privacy principles (*APPs*) applying to private and public sphere at the Commonwealth level, potentially removes one source of confusion under the previous system.

---

[193] *Privacy Act* s 7.

[194] Commonwealth Parliament, House of Representatives, *Parliamentary Debates* (No 15749, Parliamentary Debates, 12 April 2000) (D Williams, Attorney-General). At the time, the aim of the *NPPs* was to encourage private sector organisations and industries, which handled personal information, to develop and implement privacy codes of practice (see *Privacy Act* s 18B, Privacy Codes). These have now been replaced by the *APPs*.

[195] The key to the new legislative scheme is the 13 *APPs*, which set-out the legal obligations of both public and private sector for collection, storage, access and disclosure of personal information. In March 2014, the *APPs* replaced the 11 *IPPs* and 10 *NPPs*. The 13 *APPs* broadly deal with the collection, use and disclosure of personal information, and rights to access and corrections. The 13 *APPs* consist of: 1) open and transparent management of personal information; 2) anonymity and pseudonymity; 3) collection of solicited personal information; 4) dealing with unsolicited information; 5) notification of the collection of personal information; 6) use and disclosure of personal information; 7) direct marketing 8) cross-border disclosure of government related identifiers; 9) adoption, use and disclosure of government-related identifiers; 10) quality of personal information; 11) security of personal information; 12) access to personal information; 13) correction of personal information.

[196] See *APPs*, above n195.

It also introduced general provisions which rewrite the credit reporting provisions and provide for more comprehensive credit reporting, together with new provisions on privacy codes. Further, it clarified and strengthened the functions of the Australian Privacy Commissioner.[197]

The Government views the *Privacy Act* as the 'cornerstone of the privacy protection framework'[198] and represent a:

> Streamlined and harmonised set of obligations that draw on the existing principles; ensure that standards also take into account an individual's reasonable expectations around the handling of their information and to ensure that regulations strike a balance between the public's and individual's interest in efficient and effective service delivery and public safety.[199]

V. STATE AND TERRITORY STATUTORY DEVELOPMENT IN HEALTH AND INFORMATION PRIVACY

All state, territory and federal jurisdictions possess, to a lesser or greater extent, authority to govern and make laws in Australia. Constitutional limitations, which often result in law fragmentation, constitute a significant problem for harmonising state, territory and federal healthcare privacy protection. This is because the constitutional framework does not have one national health system; it has multiple systems. Recognising jurisdictional limitations and the impact of state and territory health and privacy laws provides essential, foundational bases for fully

---

[197] Department of Parliamentary Services, Mary Anne Neilsen *Privacy Amendment (Enhancing Privacy Protection)* Bill 2012 Law and Bill Digest No. 20, 2012-2013, 18 September 2012, 5-6.

[198] Joe Ludwig, Cabinet Secretary, *Companion Guide to Australian Privacy Principles* (Department of Parliamentary Services No 6, Parliament of Australia, 2006); see also, OAIC, *Australian Privacy Principles Guidelines: Privacy Act 1988* (OAIC Privacy Fact Sheet 17, date of initial publication: February 2014, revised 1 March 2014).

[199] Department of Parliamentary Services, Mary Anne Neilsen, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Law and Bill Digest No. 20 of 2012-2013, Parliamentary Library, 18 September 2012.

understanding ongoing federal involvement, progress and challenges in the new, national, electronic healthcare privacy regime in Australia.[200]

At the state and territory level, Tasmania, Victoria, New South Wales, Queensland and the Northern Territory have separate privacy legislation.[201] In addition some states and territories such as Australian Capital Territory, New South Wales and Victoria have introduced specific legislation dealing with health records.[202] However, the states and territories share commonality in respect of information privacy rights. These jurisdictions traditionally provide a regime for the responsible collection and handling of personal information.[203] Alongside privacy legislation each jurisdiction has freedom of information legislation that deals with accessing information held by state or territory government agencies and organisations. [204]

The complexity of the legislation surrounding information privacy in different jurisdictions across Australia can be demonstrated by the *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Act 2001*

---

[200] See Victorian Privacy Commissioner, 'Federal Privacy Law Changes Welcome but Does Not Affect Victorian Privacy Legislation' (Media Release, 21 March 2014); Blackshield and Williams, *Australian Constitutional Law and Theory*, above n5. Constitutionally, the responsibility for healthcare is retained by the states and territories under their 'residual' powers: at 125. See also Constitutional limitation in s109 of the *Constitution,* where 'in those jurisdictions where statutory regime is stricter, state or territory law may prevail, provided it is not inconsistent with the Commonwealth legislation … where there is an inconsistency between a Commonwealth and state/territory Act the Commonwealth law prevails and the state law is invalid to the extent of the inconsistency.'

[201] *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic)); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Information Act 2002* (NT).

[202] *Health Records (Privacy and Access) Act 1997* (ACT); *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic).

[203] *Information Act* (NT); *Freedom of Information Act 1991* (SA); *Right to Information Act 2009* (Qld); *Freedom of Information Act 1991* (Tas); *Freedom of Information Act 1992* (WA).

[204] See *Freedom of Information Act 1991* (Tas); *Freedom of Information Act 1989* (NSW); *Freedom of Information Amendment Act 20042* (Qld); *Freedom of Information Act 1992* (WA); *Freedom of Information Act 1991* (SA); *Freedom of Information Act 1982* (Vic); *Freedom of Information Act 1989* (ACT); *Freedom of Information Act 1982* (Cth).

(NSW), *Information Privacy Act 2000* (Vic) and *Health Privacy Act 2001* (Vic) legislation,[205] which each contain privacy standards that regulate the way NSW and Victoria agencies handles personal information. For example, the *Health Records and Information Privacy Act 2002* implements a privacy regime for health information in NSW private and public sector and contain 15 Health Privacy Principles (HPPs) that outline how health information must be collected, stored, used and disclosed.[206] Along similar lines as NSW, the Victorian *Information Privacy Act 2000* (Vic) covers the handling of personal information (not health information) in the state public sector.[207] The Act encompasses 10 Information Privacy Principles (IPPs) and are comparable to the old *NPPs* in the *Privacy Act*. Health records in Victoria are found in the *Health Records Act 2001* and contain 11 Health Privacy Principles (HPPs), which covers how health information in Victoria is collected, stored used and disclosed, the Act is administered by the Office of the Health Services Commissioner.

The Commonwealth Australian Privacy Principles (*APPs*) interact with state and territory laws, providing a complex web of prohibitions on, and exceptions to personal information collection, use and disclosure.[208] Notwithstanding, the *APPs* are similar but not identical with the HPPs in New South Wales and the NPPs in Victoria in that health information ('sensitive information' in the HPPs and NPPs) 'may be

---

[205] Note health records are excluded from the ambit of the *Privacy and Personal Information Protection Act 1998* s4A.

[206] See, ALRC, Discussion Paper 108, above n71: at 166-167.

[207] Note health records are excluded from the ambit of the *Information Privacy Act 2000* (Vic) s3.

[208] See s109 of the *Constitution* where 'in those jurisdictions where the statutory regime is stricter, the state or territory law may prevail, provided it is not inconsistent with the Commonwealth legislation.' See generally Danuta Mendelson, "Travels of a Medical Record and the Myth of Privacy" (2003) 11 *Journal of Law and Medicine* 136.

used for the purpose for which it was collected, or for a secondary purpose where it is directly related, and a person would reasonably expect it to be used in that way.'[209] However, in the Australian Capital Territory (ACT) Privacy Principles (PPs) 'require only that the secondary purpose be "directly related"' to the purpose.[210] This slightly 'different' wording in the principles may result in health professionals, healthcare providers and researchers in different state jurisdictions having to comply with both sets of principles (state and *APPs*).[211]

As noted, the legislation in various jurisdictions across Australia may differ, even in recognising how many privacy principles are covered and the length of time public records are kept.[212] For instance, Commonwealth legislation, such as the *Archives Act 1983* (Cth), differs from its state equivalent in that it is drafted specifically so that it dovetails with the *Freedom of Information Act 1982* (Cth). Its provisions concerning access are considerably more detailed and adopt a wider scope than the state legislation.[213] However, fundamentally the Commonwealth and state legislation share certain similar characteristics, such as specific statutory requirements for the staff of government health authorities to respect the confidentiality of patients whom they treat, as well as general privacy provisions.[214]

---

[209] See White, McDonald and Willmott, *Health Law in Australia*, above n50: at 390.

[210] Ibid.

[211] See Victorian Privacy Commissioner, 'Federal Privacy Law Changes Welcome But Do Not Affect Victorian Privacy Legislation' (Media Release, 21 March 2014).

[212] For instance, New South Wales has 15 *HPPs*, whereas Victoria has 10 privacy provisions.

[213] See Moira Paterson, *Freedom of Information and Privacy in Australia* (LexisNexis, 2005). Paterson notes that the scope of the *Archives Act 1983* (Cth) is more extensive than the state legislation and is subject to wider merit review: at 212; see also Review Process State Records New South Wales, *Issue Paper: Review of the State Records Act 1998* (2004).

[214] For instance, the *Healthcare Act 2008* (SA), *Health Administration Act 1982* (NSW), *Health Services Act 1988* (Vic) and the *Privacy Act 1988* (Cth) provide that all Commonwealth and state officers have

A *Related Legislation*

When exploring healthcare privacy, it is important to also consider a plethora of other related state and territory legislation that impact on the area. While most of this related legislation is unique to its own state or territory jurisdiction, it does share many similar characteristics with all other states and territories, in that it generally complements existing Commonwealth legislation. Included in state and territory legislation is Freedom of Information Acts,[215] which forms a vital part of a broader network of laws, both formal and informal.

Other laws that contribute and affect the overall objective of transparency such as transparency of the executive branch of government include: information privacy laws, public records laws, laws which require administrative decision-makers to provide reasons for their decisions and whistle-blower protection laws.[216] In turn, these laws enhance the accountability of Parliament, including the offices of the Ombudsman and Auditor-General.

---

obligations to keep records confidential. Procedural problems arise when it comes to information privacy complaints procedures, as these mechanisms may differ significantly between states and Commonwealth jurisdictions.

[215] See Freedom of Information legislation, above n206. Likewise, there are a number of instances across Australia (in states and territories) that permit or require, in certain circumstances, the disclosure of confidential information. For example, *Public Health Act 2010* (NSW); *Health Administration Act 1982* (NSW) ss20E-G, 22 and 23; *Public Health Act 1997* (Cth) s69; *Health Act 1958* (Vic) s 128; *HIV/Aids Preventative Measures Act 1993* (Tas); *Health Services Act 1988* (Vic). These Acts are similar across the different states and territories.

[216] See *Ombudsman (Northern Territory) Act 1977* (NT); *Ombudsman Act 2001* (Qld); *Public Records Act 2002* (Qld); *Ombudsman Act 1972* (SA); *State Records Act 1997* (SA); *Ombudsman Act 1978* (Tas); *Archives Act 1983* (Tas); *Ombudsman Act 1973* (Vic); *Public Records Act 1973* (Vic); *Whistleblowers Protection Act 2001* (Vic); *Whistleblowers Protection Act 1994* (Qld); *State Records Act 2000* (WA); *Public Finance and Audit Act 1983* (NSW); *Protected Disclosures Act 1994* (NSW); *States Records Act 1998* (NSW); *Ombudsman Act 1974* (NSW).

The Health Complaints Agencies in each state and territory may also address healthcare complaints that raise questions about the safety and quality of health services, and thus may incidentally field concerns about privacy breaches (which generally would then be referred out to the appropriate agency).[217] For example, complaints notification requirements may differ between the different states, in Queensland, all complaints and notifications about Queensland-based registered health professionals are referred to the Queensland Health Ombudsman.[218] Whereas, New South Wales chose not to adopt the national law in its entirety, arguing that it would not ensure 'the maintenance of a strong, accountable and transparent disciplinary and complaints system in New South Wales.'[219] Consequently, state complaints procedures can still result in some inconsistency between Commonwealth, state and territory health privacy protection laws across Australia.[220] These Acts may widen the scope and opportunities of resolving, investigating and prosecuting complaints about healthcare in some, but not all, jurisdictions.[221] However, the 2009 national adoption of the Health Practitioner Regulation National Law across Australia

---

[217] See, for example, *Health Quality and Complaints Commission Act 2006* (Qld); *Health Complaints Act 1995* (Tas); *Health Care Complaints Act 1993* (NSW).

[218] See *Health Ombusman Act 2013* (Qld) s68. The Queensland Ombudsman can issue a prohibition order prohibiting the delivery of services or imposing restrictions on the delivery of services. For example, an order may be issued if the health professional's conduct, performance or health means they pose a serious risk and it is necessary to issue the order to protect public health and safety.

[219] New South Wales, Legislative Assembly, *Parliamentary Debates* No 18872-18874, 28 October 2009 (Carmel Tebbutt, Minister of Health)).

[220] See, for example, *Queensland Ombudsman Act 2013* (Qld).

[221] See Australian Health Practitioner Regulation Agency ('*AHPRA*'), *Delegations Under the National Law* (LPN 22, 3 February 2014); *AHPRA*, *Court or Tribunal Power to Stay a Board Decision* (LPN 21, 18 October 2013); Tribunals in Victoria, Australian Capital Territory, Queensland and Western Australia have statutory powers to grant stays. The New South Wales Health Care Complaints Commission has a Charter to resolve, investigate and prosecute complaints about healthcare under the *Health Care Complaints Act 1993* (NSW).

has greatly contributed to the overall coordination and 'harmonisation' of national regulation of healthcare providers and health care complaints processes.[222]

To conclude, agreement between the federal, state and territory governments towards national consistency and 'harmonisation' laws, in relation to health reform and continuing individual privacy protection, has resulted in a new era of national cooperation between Australian governments across Australia.[223] Over the last decade, this level of cooperation has resulted in new Commonwealth laws and regulations in the healthcare privacy area. Nevertheless, there remains a level of caution as some states are not convinced that the federal Government will continue to provide adequate individual privacy protection, particularly in relation to online information technology advances.[224]

VI. DEVELOPMENTS IN THE NEW ELECTRONIC HEALTHCARE REGIME

Since the late 1990s onwards, the federal government, with state and territory government cooperation, has taken a very active leadership role in introducing and implementing a new electronic healthcare regime in Australia.[225] As a result of this cooperation between the different governments, significant advances in health and privacy legislative and regulatory reform have been introduced by the federal

---

[222] See, for example, *Health Practitioner Regulation National Law 2009* (Cth); *Health Practitioners Regulation National Law Act 2009* (NSW); *Health Practitioner Regulation National Law Act 2009* (Queensland); *Health Practitioner Regulation Act 2009* ((Vic).

[223] See, for example, COAG, *Australian Health Ministers Cooperation towards National Health Care* (2001); COAG, *National Healthcare Agreement* (2011); COAG, *National Healthcare Agreement 2011-2013*.

[224] ALRC, Report 108, above n71: at 499.

[225] See National Health Information Management Advisory Council, *A Health Information Action Plan for Australia* (2nd ed, 2001); National e-Health Transition Authority *('NEHTA')*, *Frontiers in Healthcare Delivery* (2007); see chapter 2, pp38-68 for a detailed discussion on health services.

Government.[226] At the *EPR* and e-health conception stage, all Australian governments agreed that to sustain 21st century healthcare services in Australia, the introduction of electronic healthcare delivery systems must be coordinated by the federal Government, in order to achieve greater national consistency and harmonisation of laws across Australia.[227]

Major contributions by the federal Government to legislative privacy reform and *PCEHR* e-health systems implementation include recent amendments to the *Privacy Act*, enactment of new legislation such as the *Healthcare Identifiers Act 2010* (Cth) as well as since abandoned 'proposed' statutory changes, including a *Statutory Cause of Action for Serious Invasion of Privacy*.[228] Legal reform in the privacy and *PCEHR* healthcare area is also influenced by numerous government reports over the last decade.[229] Government generated and privately commissioned reports provide significant insight into the overall objectives and ongoing evolution of privacy and *PCEHR* healthcare privacy legislation in Australia.[230]

A *Commonwealth Legislation Supporting PCEHR Implementation*

---

[226] See NEHTA, *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System* (September 2011).

[227] See chapter 2, pp38-68 for a detailed discussion on health services; Australian Government, *National Health Reform* (2011).

[228] See earlier chapter, pp146-163 discussion on common law privacy development.

[229] Australian Government, *Healthcare Identifiers and Privacy: Discussion Paper on Proposals for Legislative Support* (2006); Australian Government, *Personally Controlled Electronic Health Records System: Legislation Issues Paper* (2008); NEHTA, *Concepts of Operations*, above n226.

[230] See chapter 2, pp38-67 discussion on federal Government e-health policy development; see, for example, ALRC, Discussion Paper 108, above n71; Australian Government, *Concepts of Operations,* above n226; National E-Health and Information Principal Committee, Deloitte, *National E-Health Strategy* (30 September 2008).

The *Healthcare Identifiers Act 2010* and the *PCEHR Act 2012* represent Commonwealth legislation supporting a national, coordinated approach to the implementation of a new electronic healthcare regime in Australia. The *Healthcare Identifiers Act* is a foundational piece of Commonwealth legislation, because it enables 'accurate identification, retrieval and information sharing' throughout the healthcare system.[231] The purpose of the *Healthcare Identifiers Act* is to establish a national healthcare identifier system for patients, healthcare providers and healthcare provider organisations, as well as setting out the purposes for which healthcare identifiers can be used. In addition to this Act, other supporting legislation and regulations were also introduced: *Healthcare Identifiers (Consequential Amendments) Act 2010* (Cth) and the *Healthcare Identifiers Regulations 2010* (Cth).

Under s 9 of the *Healthcare Identifiers Act*, Medicare Australia is appointed as the Service Operator of the system. The Service Operator is authorised to assign healthcare identifier ('*HI*') numbers to both health consumers and healthcare providers and manages the system. The assignment by Medicare of a *HI* number to an eligible consumer is mandatory. Key definitions are located in Part 1 of the *Healthcare Identifiers Act* and include: 'healthcare', 'healthcare identifier', 'healthcare provider', 'health recipient' and 'healthcare information'.

The definitions of 'healthcare provider' in s 5 of the *Healthcare Identifiers Act* and 'healthcare services' in s 6 of the *Privacy Act* must be read together and provide

[231] See Danuta Mendelson, "Healthcare Identifiers Legislation: A Whiff of Fourberie" [2010] 17 *Journal of Law and Medicine* 660.

exceptionally wide meanings to each term.[232] Both the *Privacy Act* and the *Healthcare Identifiers Act* allow for the possibility (particularly in the regulations) of an increasing number of people and organisations claiming access rights to personal health information; this is problematic for consumer healthcare information privacy because it represents an unanticipated source of access to medical records.[233]

The *PCEHR Act 2012* (Cth) provides for a system of access to electronic health records and related purposes. The object of the Act is to enable the establishment of the personally controlled electronic health record system and provide its regulatory framework, including an entity that is responsible for the operation of the *PCEHR* system to:

> (a) help overcome the fragmentation of health information; and
> (b) improve the availability and quality of health information; and
> (c) reduce the occurrence of adverse medical events and the duplication of treatment; and
> (d) improve the coordination and quality of healthcare provided to consumers by different healthcare providers.[234]

The *PCEHR Act* outlines the *PCEHR* system infrastructure set up and defines the legal requirements for collecting, using and disclosing patient information. The Act also sets out the proposed management and governance arrangements for the *PCEHR* system.[235] Further it regulates the function of the System Operator and registration by the System Operator of consumers, healthcare provider organisations, repository

---

[232] *Healthcare Identifiers Act 2010* (Cth) s5: 'Healthcare provider means: (a) an individual healthcare provider; or (b) a healthcare provider organisation.' *Privacy Act* s6: 'Healthcare services means: (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual on the person performing it: (i) to access record maintain or improve the individual's health; or (ii) to diagnose the individual's illness or disability or suspected illness or disability; or (iii) treat the individual's illness or disability or suspected illness or disability; or (b) the dispensing on prescription of a drug or medicinal preparation by a Pharmacist.'

[233] See, for example, naturopaths, herbal medicine practitioners, masseurs.

[234] *PCEHR Act 2012* (Cth) s3.

[235] See chapter 6, pp184-234 for discussion of the *PCEHR* and e-health governance proposal.

operators, portal operators and contracted service providers. The *PCEHR Act* states that the System Operator is authorised to use or disclose health information included in a consumer's *PCEHR* if the System Operator 'reasonably believes that the use or disclosure is reasonably necessary for one or more [of the listed] reasons' such as 'the prevention, detection, investigation, prosecution or punishment of criminal offences'.[236] The implication of this section is that it provides wide latitude of control to the System Operator in relation to disclosure of *PCEHR* information.

The *PCEHR Act* established two new advisory bodies to NEHTA and the Department of Health and Ageing—the *Jurisdictional Advisory Committee* and the *Independent Advisory Council*—further examined in chapter 6 of the thesis.[237] The Act requires that the Minister makes *PCEHR* Rules and that he or she 'must consult the Committee and Council' about new or altered Rules.[238] However, the legislation also states that the validity of the Rules (new or established) is not affected by the Minister's failure to consult with *Committee* or *Council* about the Rules. This 'loophole' gives rise to the potential that the Minister can effectively 'by-pass' overview processes when introducing new *PCEHR* Rules. Consequently, this situation effectively fails to provide genuine oversight of the Minister's decision-making powers in the *PCEHR* area and is of concern to the overall transparency and democratic functioning of the *PCEHR* system.

B *Privacy Amendment (Privacy Alerts) Act 2013 (Cth)*

---

[236] *PCEHR Act 2012* s70 (5).

[237] See *PCEHR Act 2012* s2 (a)-(b), s18, s24.

[238] *PCEHR Act 2012* Part 2 Division 1, s16, Divisions 2, 3 and 4.

The latest addition to strengthening privacy protection is the *Privacy Amendment (Privacy Alerts) Act 2013* (Cth) *('Alerts Act')*.[239] Prior to the *Alerts Act* there was no legal obligation on entities to notify the Information Privacy Commissioner, or any individuals whose personal information had been compromised; this situation was rectified by this new privacy amendment.[240]

'Data breach notification' is a topical concern around the world, especially in relation to identity theft and identity fraud, which have been the main issues driving the development of new laws in this area.[241] As part of its first stage response, the Australian Government decided not to implement the initial *ALRC* recommendation about mandatory breach notifications.[242] However, due to a number of high profile data hacking cases, including the hacking of the ABC's website, and breaches at Telstra, Medvet and Sony PlayStation, the government brought the introduction of this legislation forward. [243]

Mandatory 'data breach notification' commonly refers to:

> A legal requirement to provide notice to affected persons and the relevant regulator when certain types of personal information is accessed, obtained, used, disclosed, copied, or modified by unauthorised persons. Such unauthorised access may occur following a malicious breach

---

[239] The first Parliamentary reading of the *Alerts Act* took place on 29 May 2013. It had its second reading and moved through Senate on 17 June 2013 and came into effect in March 2014.

[240] At the time, *IPP* 4 and *NPP* 4 (now superseded by the *APPs*) required agencies and organisations to take reasonable steps to maintain the security of the personal information they held. A voluntary guide for entities, giving advice on how to handle a data breach, was developed in 2008 by the Privacy Commissioner (*OAIC, Data Notification: A Guide to Handling Personal Information Security Breaches* (2008, revised late 2011)).

[241] ALRC, Report 108, above n71: Para 51.1.

[242] See Mary Anne Neilson, *Privacy Amendment (Privacy Alerts) Bill 2013*, Law and Bills Digest No. 146, 2012-2013, 19 June 2013; Australian Parliament, House of Representatives, *Explanatory Memorandum*, Privacy Amendment (Privacy Alerts) Bill 2013, 2013: at 6.

[243] See Department of Parliamentary Services, Rhonda Jolly, *Personally Controlled Electronic Health Records Bill 2011*, Bills Digest No. 100, 2011-2012, 7 February 2012; Australian Parliament, House of Representatives, *Explanatory Memorandum*, Personally Controlled Electronic Health Records Bill 2011, 2011.

> of the secure storage and handling of that information (e.g. a hacker attack), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise.[244]

The principle behind increasing the Privacy Commissioner's mandate and overall responsibilities contained in the *Privacy Act* is considered a very positive step forward for overall governance of healthcare privacy; however there remains a pressing question of adequate resource allocation, particularly in light of the federal Government's rationalisation and devolution policy. It was noted by the *Law Council of Australia*, that while supporting the general principle of data breach notification, that this does bring forward some interesting limitations in relation to resourcing and enforcement:

> Already stretched resources … will be substantially affected by the expansion of the functions and powers of the Commissioner proposed under the Amending Act … Any mandatory notification scheme should therefore be considered in the context of the available resources at the OAIC and any subsequent limitations in its governance and policing of privacy obligations and organisations and agencies. If too great a burden is placed on the OAIC, it may be unable to effectively perform the functions conferred upon it by the Privacy Act.[245]

The above comments by the *Law Council of Australia* resonate with the thesis observation that despite current legislation, effective enforcement of individual privacy rights proposed by the previous federal Government may be compromised in the future by the lack of proper robust governance, including necessary allocation of resources to support the new laws and system.[246] This observation takes on further

---

[244] See Department of Parliamentary Services, Rhonda Jolly, *Personally Controlled Electronic Health Records Bill 2011*, Bills Digest, above n196; Australian Parliament, House of Representatives, *Explanatory Memorandum*, PCEHR Bill 2011, 2011: at 1.

[245] Law Council of Australia, *Submission to the Attorney-General's Department Discussion Paper on Australian Privacy Breach Notification* (29 November 2012); see also Mary Anne Neilson and Jonathan Chowns, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Law and Bills Digest No. 20, 2012-2013, 7 November 2012. [Notes position of major interest groups, for instance Australian Privacy Foundation, Law Council of Australia, Australian Direct Marketing Association, Victorian Privacy Commissioner, relating to main issues and key provisions (such as function creep): at 11-14].

[246] See chapter 6, pp184-234 for discussion of *PCEHR* and e-health governance issues.

relevance with the federal Coalition Government's 2014 federal *budget* cuts to health and plans to rationalise the Office of the Information Privacy Commissioner.

C *The Problem of 'Function Creep'*

During the Healthcare Identifiers Bill 2010 (Cth)'s initial consultation period, a number of worrying concerns about privacy protection emerged in relation to the introduction of individual and healthcare provider *HI* numbers.[247] These concerns included that 'such a highly reliable identifier is not usurped for purposes beyond the health system and the clinical care of individuals'.[248] At the time, the *Office of the Australian Privacy Commissioner* ('*OAPC*'),[249] noted that 'function creep'[250] had been experienced in relation to Canada's Social Insurance Number, which came to be viewed as a mode of identification, with property owners requiring its production for other unrelated situations.[251] In its submission on the Healthcare Identifiers Bill, the

---

[247] See, for example, Danuta Mendelson, "Healthcare Identifiers Legislation", above n184: at 301-40; Graham Greenleaf, 'Quacking like a Duck: The National ID Card Proposal' (2006) Compared with the Australia Card (1986-87)' (Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales (Draft only) 12 June 2006). Revised version of paper available at <http://www.cyberlawcentre.org>; Graham Greenleaf, *Submission 59* (2009): at 1-2; Senate Community Affairs Legislation Committee, Healthcare Identifiers Bill 2010 (Cth); Provisions Healthcare Identifiers (Consequential Amendments) Bill 2011 (Cth) (March 2010).

[248] Office of the Privacy Commissioner, *Submission on the Healthcare Identifiers and Privacy Discussion Paper on Proposal for Legislative Support* (12 August 2009)

[249] The Office of the Privacy Commissioner is also referred to as the Office of the Australian Information Commissioner.

[250] Graham Greenleaf, "Access all Areas: Function Creep Guaranteed in Australia's ID Card Bill (No 1)" [2007] *University of New South Wales Faculty of Law Research Series* 11. ' The term 'function creep' 'is said to occur when customer or patient data is stored for one purpose, such as medical records, but someone figures out another use for it, or wants to share the data with another party. That is, when the original intention for storing information is expanded to gain extra information about the subjects or to use the information for an entirely different purpose'; see R LeMay, 'Hackers on Medicine Smartcard Waiting List' *ZD Net* (online) <http://www.zdnet.com.au/hackers-on-medicare-smart-card-waiting-list> (viewed on 24/2/2005); see also S Mitchell, 'Privacy Warning on Medicare Smartcard' *The Australian* (Australia), 22 November 2005, 2.

[251] See OAPC, *Submission on the Healthcare Identifiers and Privacy: Discussion Paper on Proposal for Legislative Support* (2009).

OAPC provided overseas examples of this type of 'function creep'.[252] The *OAPC* observed:

> Property owners asked for it on apartment rental applications, video stores required it as security for movie rentals, universities and colleges requested it on their application form and pizza places even used it as a customer number for their delivery system.[253]

The long-term implication for Australian healthcare consumers of increasing 'function creep' is that, unless individual privacy protection law is both *unambiguous* and *strong* in its purpose to protect individual healthcare privacy requirement, there remains a high possibility that, despite legislative prohibition, the *HI* number and information will be used for non-health related management and commercial purposes.[254]

As Daniel Solove explains, this type of 'function creep' is especially problematic where the government is strongly committed to ongoing health commercialisation and privatisation, extending personal health information access to a growing number of local and international, public and private sector, healthcare organisations and researchers, who operate in an environment where corporate and business interests typically advocate 'free flow' deregulation of all information.[255] This is particularly

---

[252] OAPC, *Submission on the Healthcare Identifiers and Privacy*, above n248.

[253] Ibid.

[254] OACP, *Submission on the Healthcare and Privacy*, above n252 [where it is argued by the thesis that the submission observations made by the *OAPC* continue to resonate in 2015], with the federal Coalition Government arguing for the expansion of *HI* number information usage to include general commercial interests, and the argument that *PCEHR* and e-health governance should increasingly be managed by the private sector.

[255] See Daniel Solove, *The Digital Person* (New York University Press, 2004) 1-9; see also Brian Murchison, 'Revisiting the American Action for Public Disclosure of Private Facts' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press, 2006): at 32. Review Panel, Richard Royle, Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* (December 2013) ('*Royle Review*'). The *Royle Review*, recommendations (at time of writing February 2015) are yet to be accepted by the federal Government; *Coalition Policy on E-Government and Digital Economy*, above n60, make it highly probable that *HI* numbers will be extended

pertinent given the 2013, *Royle Review* recommendation that would allow the expansion and use of HI numbers.[256] This issue is further discussed in chapter 6.

VII. CONCLUSION

The above analysis of the legal dimension highlights the growing importance of privacy and law and its continuing relevance to individual healthcare privacy protection. As recently highlighted by the ALRC, 'privacy is a fundamental value worthy of protection,' that 'privacy laws should be adaptable to technological change', and the law should be 'consistent and coherent,' as well as 'clear and certain.'[257] The chapter discussion also demonstrates the limitations surrounding federalism, common law and statutory law, particularly in the modern digital information environment. In Australia, the constitutional framework (federation) continues to result in legal fragmentation and adds to the complexity of laws in both the health and privacy domain. This occurs mainly because State and Territory Governments continue to feel pressure to fill in the 'gaps' in relation to individual privacy protection, as they attempt to grapple with emerging legal and moral privacy concerns that arise in a modern, global, information economy.

The issue of state/territory and federal cooperation and 'harmonisation' of laws is also threatened with the current federal government at risk of compounding

---

beyond their original promised purpose and be used for general commercial purposes (outside of healthcare services: at 15-18; See chapter 7, pp250-255 — this chapter details the *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013) recommendations and *Coalition's Policy for E-Government and the Digital Economy*, above n60: at 3.

[256] *Review of the Personally Controlled Electronic Health Record,* ibid.

[257] ALRC, Discussion Paper 80, above n46, see Principle 1, Principle 5, Principle 6 and Principle 7: at 28, 32, 33.

the problem of fragmentation in health and privacy as it pursues a policy of economic restraint, decentralisation, and deregulation of healthcare delivery services. It is foreseeable that given the current federal Government's vision of global commercialisation and privatisation of healthcare systems, that earlier collaboration trends will be jeopardised as Australian states and territories individually respond to continuing pressure to regulate this area.

The following chapter 6 continues the analysis of a new electronic healthcare regime in Australia by expanding upon the statutory and governance dimension and further exploring alternative ways to best protect Australian individual and collective privacy interests and rights.

CHAPTER 6

ENHANCING HEALTHCARE PRIVACY: E-HEALTH TECHNOLOGY AND GOVERNANCE MEASURES

Along with recent legislative changes, outlined in the previous chapter, the aim of this chapter is to further extend the analysis of the Australian Government's *PCEHR* and e-health privacy solutions, by exploring various proposals for the adoption of privacy-friendly technical and *PCEHR* governance measures, as well as identifying their application and progress thus far. The analysis centres on newly arising privacy governance concerns such as ongoing e-health governance development; current private and public regulatory overview; government health privatisation and commercialisation policy; the consumer *PCEHR* 'opt-in' consent model; and security and storage of healthcare information data. The chapter also emphasises recent recommendations made to the federal Health Minister by the review panel in *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*').[1]

In order to appreciate the current modern Australian political and economic 'shift' in healthcare governance discourse and its increasing importance on the day-to-day management and lives of ordinary citizens, the chapter adopts a multi-dimensional, political, economic and social contextual perspective for exploring emerging privacy challenges. These include the rise of modern-day communication

[1] See Review Panel, Richard Royle, Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013).

'networks', democratic theory development, civil liberties rights, as well as constructing modern era governance in light of growing globalisation influences, which all impact on the very fabric of liberal democratic societies, such as Australia.[2] The analysis of earlier Australian Government *PCEHR* reports and legislation,[3] along with recent recommendations, is fundamental to understanding e-health governance arrangements because *PCEHR* proposals enhancing personal privacy tend to treat these arrangements 'as an end in itself' utility problem, rather than an essential part of a democratic process.[4]

Crucially, so far as the future of *PCEHR* and e-health governance development is concerned, the chapter argues that the focus of attention, or analytical lens, is on how best to stimulate a form of deliberative democracy within the arrangements — thus achieving an overall balance that, it is suggested, law, technology and market mechanisms cannot achieve on their own. This is the basis for the thesis contention that a new *Council* with multiple governance oversight functions, represents a vital democratic reform mechanism for addressing ongoing e-health governance deficiencies. The *Council* being argued for in the thesis is designed to foster an inclusive governance approach that promotes democratic citizen participation and

[2] See Simon Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001): at 143.

[3] See chapter 5, pp124-182 for discussion on Commonwealth PCEHR legislation; see e.g. *Healthcare Identifiers Act 2010* (Cth); *Personally Controlled Electronic Health Act 2012* (Cth).

[4] See Evgeny Morovoz," The Real Privacy Problem" (22 October 2013) 116(6) *MIT Technology Review* 32-43.

government transparency, connecting with wider ongoing democratic, political and economic accountability in the evolving modern global economic environment.[5]

Chapter 3 critiqued various philosophical and theoretical arguments concerning the rise of modern utility technology (such as computer technology, social media and *APP* networking reliance), as it impacts on *PCEHR* and privacy development in Australia.[6] Nevertheless, it is worth reiterating that the rapid rise of the knowledge and information economy, preferences for neoliberal economic arrangements and forms of governance, together with the push towards marketplace globalisation, further complicates realising *PCEHR* privacy protections and accountability through democratic participation.

I. MODERN DAY CHALLENGES TO DEMOCRACY

The evolution of the 'state' is closely bound up with ideals of liberal democracy, which promotes the rule of law, separation of powers, the role of citizens and generally, democratically elected political representatives.[7] The modern-day threat to democracy in the present, economic context occurs because the traditional division between business focus on profits (economics) and state systems (administration), to provide public good, is challenged by non-governmental actors in an increasingly global environment.[8] Another significant influence on traditional, liberal, democratic

[5] See chapter 7, pp255-260 for overview and details of an *Independent Council* (Council).

[6] See chapter 3, pp70-98 for technology analysis.

[7] See Robin Creyke and John McMillan, *Control of Government Action* (LexisNexis, 3rd ed, 2012). Creyke and McMillan outline the historical the development of Westphalia ('state') system of Government and its relationship with accountability mechanisms: at 3-4.

[8] See Eugeny Morozov, "The Real Privacy Problem", above n4: at 32.

ideals, such as election of government and centralised policy making, is the formation of a decentralised global 'network' system based upon the 'free' flow of information.[9]

The rise of globalisation theory, according to John Dryzek, inverts the relationship between domestic and international factors.[10] For globalists, the key influences on the state are now international, and consequently, domestic forces are downplayed. What this implies is that global systems are regarded as fundamental. These systems may be markets, 'networks' or may involve communications (such as internet), or may mix political, economic and cultural aspects. Thus, globalists tend to insert assumptions about the importance of international flows, systems and networks compared to their domestic counterparts.[11]

Further, Morozov's privacy and citizen right analysis contends that another central threat to democracy is the power of modern-day communication media, such as social media. He argues that social media will satisfy what people think they need and as a consequence people will become complacent and cease to question the real driving motive beyond the virtual fantasy world. Noting that 'smartphone and other computer applications have the potential to direct our behaviour, remind us when we have erred and blunt our capacity to challenge society.[12]

---

[9] See Ramesh Subramanian and Eddan Katz, 'Perspectives on the Global Flow of Information' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University, 2011): at 1.

[10] See John Dryzek and Patrick Dunleavy, *Theories of the Democratic State* (Palgrave Macmillan, 2009) 221.

[11] See Ramesh Subramanian, et al, *The Global Flow of Information*, above n9; John Dryzek, et al, *Theories of the Democratic State*, above n10: at 310; see also Penelope Simons and Audrey Macklin, *The Governance Gap* (Routledge, 2014).

[12] See Evgeny Morovoz, "The Real Privacy Problem", above n4: at 32.

Morozov speculates that human complacency and acceptance about technology constitutes a very real threat to established, democratic processes and citizen privacy rights,[13] because 'we can now be pinged whenever we are about to do something stupid, unhealthy or unsound.'[14] He imagines the new digital infrastructure as 'thriving as it does on real-time data contributed by citizens, allowing technocrats to take political, with all its noise, friction, and discontent, out of the political process.'[15] It replaces 'the messy stuff of coalition-building, bargaining, and deliberation with the cleanliness and efficiency of data-powered administration.'[16]

II. TOWARDS DELIBERATIVE DEMOCRACY

In order to address perceived democratic deficiencies in an increasingly global, political, economic and social environment, some modern theorists ascribe to 'deliberative democracy' as an alternate form of democratic process protection.[17] Accordingly, the deliberative model of democracy is able to acknowledge the contribution of both state and non-state actors (including citizens) to global governance, that emerge outside the traditional realm of institutionalised politics. A key assumption of the deliberative model of democracy is the idea that politics does not exclusively take place in official, governmental institutions, but already starts at the level of deliberating, civil society associations. Regulatory activities of

[13] See Andreas Georg Scherer and Guido Palazzo, "The New Political Role of Business in a Globalised World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democrat" (4 June 2011) 48*Journal of Management Studies* 4.

[14] Evgeny Morozov, "The Real Privacy Problem", above n4: at 32; see also chapter 3, pp78-79 for discussion on 'social media' technology.

[15] Evgeny Morozov, "The Real Privacy Problem", above n4: at 32-33.

[16] Ibid.

[17] See Scherer and Palazzo, "The New Political Role in a Globalised World", above n13: at 917; Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 215.

governments should be connected to those processes of public-will formation. Thus, democratic legitimacy is created by the strengthened links between the decisions in the political institutions and the processes of public-will information, as driven by non-governmental organisations, civil movements and other civil actors 'who map, filter, amplify, bundle and transmit private problems, values and needs of the citizens.'[18]

Consequently, with non-government actors becoming more powerful and through their engagement in the process of self-regulation, they become subjects of new forms of democratic processes: control and legitimacy. Whilst liberal models of democracy place emphasis on the beneficial outcomes of the political process, deliberative democracy turns on the argumentative involvement of citizens in the decision-making processes themselves. Certainly, the introduction of the proposed *Council* as a political citizen forum within the proposed (but modified) governance, institutional model would promote a deliberative, democratic approach by establishing a citizen 'voice' in present and future institutional, decision-making activities. Given that effective citizen representation falls short of expected participation in the governance process, and is arguably denied in the *Royle Review* model discussed later in the chapter, the introduction of the *Council* seeks to re-establish and re-affirm citizen 'voice' and active participation in present and future institutional, decision-making activities.

[18] See Jurgen Habermas, 'Three Normative Models of Democracy' in Jurgen Habermas (ed), *The Inclusion of the Other: Studies in Political Theory* (Cambridge MIT University Press, 1998): at 239-52; see also Jurgen Habermas, *The Postnational Constellation* (Cambridge University Press, 2001); see also Scherer and Palazzo, "The New Political Role of Business in a Globalised World", above n13: at 918.

Deliberation is a recognised communication process whereby individuals reflect upon their own views in light of what others have to say, ideally in a context free from coercion, deception and manipulation. The highlighting of deliberation means that 'talk-centric democratic theory replaces voting-centric democratic theory — though voting is not ruled out.'[19] Deliberative democracy is not just a political theory; it has inspired a wide range of social reforms in liberal democracies in recent years.[20]

'Deliberative democracy' is grounded in an assumption that individuals emphasise their capacity to reflect upon their own preferences, values and judgments in their participation in political dialogue with other individuals. As noted, rather than a focus upon the electoral connection between the state and public spheres, there are a number of other mechanisms for the transmission of public opinion and concern, apart from counting heads in an election. For instance, these might include the government's fear of political instability, leading to policy that addresses the concerns raised by, say, disadvantaged groups in society.[21] Discursive legitimacy is then secured when a public policy is consistent with the 'constellation of discourses' found in the public sphere, but only to the extent this constellation is itself under the reflective control of competent actors. Public opinion can then be thought of as the outcome of the engagement of discourses, as transmitted to the state.[22]

---

[19] Simone Chambers, "Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation" (2004) 12 *Journal of Political Philosophy* 389, 391.

[20] See, for example, Danish Board of Technology.

[21] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 216.

[22] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10; see also Julia Black, 'Critical Reflections on Regulations' (Paper Presented at Australian Society of Legal Philosophy Conference in Canberra, February 2001); see Jon Stern and Stuart Holder, "Regulatory Governance: Criteria for

In a deliberative democracy model, state and society ought to be connected by means that are themselves deliberative. Legitimacy of 'deliberative democracy' depends on 'the right, opportunity and capacity of those subject to collective decision to participate in consequential deliberation about the content of the decision in question.'[23] Citizens need to be able to participate in deliberation about a decision, rather than simply vote upon it. Applied to large and complex societies, such as Australia, however, the theory of 'deliberative democracy' immediately runs into problems of scale.

Nevertheless, there are a number of possible solutions to the scale problem. The first is to restrict the number of deliberators to, say, elected representatives. This would satisfy deliberative democrats who highlight deliberation within the legislature. The main problem which arises, when relying on elected representatives to deliver on the legitimacy claims of deliberative democracy, is that election campaigns themselves are often not very deliberative. A more democratic, non-electoral way to identify deliberating representatives is to follow the ancient Athenian model and select them by lot — just as jury pools are selected for court cases. The people selected can be representative of the population in a statistical sense, because they lack any accountability to a broader public outside the deliberative forum.[24]

Assessing the Performance of Regulatory Systems: An Application to Infrastructure Industries in the Developing Countries of Asia" (March 1999) 8 *Utilities Policy* 35; see Richard Au and Peter Croll, 'Consumer-Centric and Privacy-Preserving Identity Management for Distributed E-Health Systems' (Paper Presented to 41st Hawaii International Systems Sciences Conference, March 2008).

[23] See Bernard Manin, "On Legitimacy and Political Deliberation" (1987) 15 *Political Theory* 338, 339; see also Simons and Macklin, *The Governance Gap*, above n11.

[24] See John Parkinson, *Deliberating in the Real World: Problem of Legitimacy in Deliberative Democracy* (Oxford University Press, 2006) 218.

This concept of individual participation and action is completely different to that deployed by market liberals, who treat individual preferences as fixed and given, and view action exclusively in terms of individuals' pursuit of pre-given preferences. Elite theorists would see deliberative democracy as a sideshow, on the basis that members of the ruling elite are perfectly aware of their own interests and how to go about achieving them, without reflection from others.[25]

Some deliberative theorists have been silent on the institutional specifics of a deliberative democracy, focusing mainly on the activity of deliberation rather than its location. However, this thesis argues that the institutional design is relevant for deliberation, and the settings (outside and inside formal or informal spheres) are significant to its successful political application. Designed institutional forums, such as a *Council* proposed in this thesis, are a means of securing the direct, deliberative participation of non-government actors. Non-partisan forums involve lay citizens, recruited at random from the larger population. They are brought into an information-rich setting and given access to advocates for different sides and expert witnesses.

As noted previously, the idea is that citizens then deliberate amongst themselves on the issue and produce a set of recommendations for public policy. The number of citizen deliberators range from 10 to many hundreds (depending on the issue). Examples include consensus conferences, such as the Danish Board of Technology. Traditionally, the main issues deliberated by lay citizen forums have

[25] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 215.

focused upon genetically-modified foods; but there is no reason why this mechanism cannot be expanded to include technology and privacy rights under the proposed 'Council'. Normally, lay citizens suggest recommendations more sensitive to the risks associated with technology and privacy, than the positions taken by government and industry-dominated committees. It is recognised that lay citizens can make exceptionally good deliberators in such forums, because they are not encumbered by any prior partisanship on the issue and so approach decision-making with an open mind, amenable to persuasion.

However, a problem with 'deliberative democracy' is the recognition that not all communication is deliberative, and might include sensationists, propagandists or public relations 'spin-doctors'. A discourse is a shared language-based form that enables understanding of the world, embodying judgments, assumptions, contentions and capabilities.[26] Those who subscribe to a particular discourse can 'then recognise and process sensory inputs into coherent accounts or stories, shared in inter-subjectively meaningful fashion.'[27] Examples of shared discourse include environmental policy, human rights (such as privacy) and international global politics (e.g. the United Nations (UN), OECD and World Trade Organisation (WTO)). The engagement of discourses in the public sphere may also produce a cultural change that eventually pervades politics.

Under pluralism, market liberalism and corporatist theory, the legislature is less 'central' and so their deliberation capacities are less crucial. Of equal concern,

[26] Dryzek and Dunleavy, *Theories of the Democratic State*, above n10.

[27] See John Parkinson, *Deliberating in the Real World*, above n24.

and gaining more currency in Australian politics, is the degree of deliberativeness in the corporate institutions that integrate executive officials, business and labour federations.[28] These institutions often operate in greater secrecy than Parliament, and any deliberative qualities they do possess are attenuated by a lack of democratic representativeness of the non-governmental officials present.[29]

The thesis proposition for the introduction of the *Council*[30] to evaluate present and future *PCEHR* privacy practice and management, empowered by Parliament, with direct access to the federal Health Minister, the Standing Council on Health, and the Australian Commission for Electronic Health.[31] This recommendation for political oversight of a *Council* aligns with democratic citizen participation values and is on equal footing with other non-government and government actors proposed by the *Royle Review*.[32]

A *Pluralism Democracy*

The pluralist model of democracy involves a more complex view of political power than the standard account of representative democracy. Pluralists assume that power resides with individuals who organise themselves into pressure groups, in order to

[28] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 222; John Braithwaite, *Regulatory Capitalism* (Edward Elgar, 2008) 14-15.

[29] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 222-223; Julia Black, 'Critical Reflections on Regulations', above n22; see also Julia Black, "Constitutionalising Self-Regulation" [January 1996] *The Modern Law Review*.

[30] See chapter 7, pp255-260, which outlines and discusses the process of selection for the *Independent Council*.

[31] As proposed by the *Royle Review*, above n1.

[32] The role of a *Council* would be in line with the proposed *Independent Advisory Council* and the *Australian Commission for Electronic Health*, it would report directly to the federal Minister of Health, *Standing Council on Health* and Parliament; see chapter 7, pp238-260 structural details of a *Council* and *Royle Review* are outline in chapter 7.

assert their interests on any given issue. Under this model, governments function as neutral adjudicators, balancing the various claims and resolving problems, by developing what they take to be the most appropriate social policy.[33]

Democracy is not seen as a form of self-government, but as a political process in which individuals are able, if they want to play a significant role in influencing the government's determination of social policy. Under this model, individuals are able to participate more directly than allowed by the other models, as their participation goes beyond electoral politics or the politics of protest. Individuals can organise themselves into groups to create and influence policy by lobbying about whatever they consider important enough to justify their time and energy.[34]

Pluralism today grapples with the realities of concentrated business power, corporate partnerships, and the growing influence of technical expertise in policy making, large and complex states and networked and multi-level governance. At the same time, pluralism remains committed to dispersed power and representative government. It is considered that money must not be allowed to be the dominant good that controls the distribution of all other social goods — such as political power, healthcare, education and other areas of life.[35]

Appeals to pluralism often had to repel attacks from market liberals, who saw groups as obstructions to the public interest. Some theorists believe that the ultimate locus of collective decisions can be found in the formal institutions of the state, whilst

---

[33] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10.

[34] See Beth Gaze and Melinda Jones, *Law, Liberty and Australian Democracy* (The Law Book Company, 1990).

[35] Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 154.

others believe that the state has devolved into more informal networks. The development from pluralism to neo-pluralism involved increasing the emphasis on 'polyarchy' as a way of thinking about the closest approximation to democracy possible in the real world.

In contrast to earlier pluralists, neo-pluralists believed that inequality of influence was inevitable. This kind of imbalance of input that preoccupied neo-pluralists was between business corporations and everyone else. The level of influence by business is explained by the sheer wealth at its disposal, which means that business is able to hire the best lobbyists, conduct the best market research and engage the most persuasive spin-doctors and top lawyers to promote its cause.

B *Market Liberalism Democracy*

Market liberalism seeks to reform government, in the belief that capitalism is the optimal system for discovering and using knowledge, for securing prosperity and promoting economic and political freedom. It argues that private corporations operating under the discipline of the market can always perform service delivery and manufacturing better. By the late 1970s, market liberal theorists had built up a comprehensive, explanatory theory on state, democracy and human capabilities that accepted the assumptions about self-interested rational choice theory. New proposals by a wave of economic theorists include privatisation of state-owned enterprises, competitive bidding for private contractors to supply government services and de-regulation of the economy. Consequently, large hierarchical public systems should give way to more competitive arrangements designed to establish individual consumer control over services such as education, social insurance and healthcare.

Under this model, roughly speaking, consumers maximise their utility and private producers maximise their profits or market share. Interest groups (or firms operating in government-regulated markets) try to obtain from government a 'rent' or unearned benefit, either financed via general taxation or achieved by manipulating regulatory rules.[36] Prescriptions for engaging in this model would involve a less ideological style of managing the public sector, adopted by both left and right politicians, called 'new public management'.

This 'new' type of management has three core principles, which are all evident in the *Royle Review*, discussed later in the chapter. These principles are: disaggregation (breaking up large government bureaucracies);[37] competition (forcing public services to perform competitively in order to attract customers and finance, rather than obtaining a budget as of right);[38] and incentivisation (shifting away from professionalism or a public service ethos towards pecuniary incentives, to encourage personnel to perform better).[39] This model, alongside pluralism and potentially elite neo-pluralist sentiments, is suggested as being the most indicative description of modern-day Australian government, political and economic thinking.

C *Civil Liberties and Civil Rights*

Besides the enactment in 1901 of the *Commonwealth Constitution* and the establishment of formal courts of law, including the High Court of Australia, the complementary

[36] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 131.

[37] See *Royle Review*, above n1, Rec. 2 and 9 to dissolve NEHTA and restructure the Department of Health and the Department of Human Services: at 15-16.

[38] *Royle Review*, Rec. 9, 11 and 12.

[39] *Royle Review*, Rec. 12, 19 and 36.

system of administrative law has evolved and includes the development of additional mechanisms to facilitate review of government decision-making oversight,[40] as explained in chapter 5. Australia has developed a strong administrative regulatory governance tradition that is premised upon democracy, civil liberties[41] and long-standing principles, such as open-government and accountability.[42]

There exists a strong relational link between civil liberties, civil rights and democracy.[43] However, the scope of claims to civil liberties depends very much on the justification proffered. For instance, it can include claims made in the name of rights, to the state providing goods and services and to the state protecting the interest of individuals, where these are threatened by non-state agencies. These interpretations of the scope of the guarantee that the state should provide for its citizens, turns in part, on 'the vision of democracy held by the proponents of the right or liberty and in part on the theoretical basis upon which claims to rights and liberties are made.'[44]

Because the traditional focus of most liberals is a commitment to promoting individualism (negative liberty protections against intrusions on individual rights), the distributive welfare assertion that the state provide individuals with sufficient

---

[40] See for example, Commonwealth Administrative Review Committee, Tribunals, Ombudsman

[41] See Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34. According to Gaze and Jones, the concern of civil liberties is the position of the individual in society': at 2, and that 'the freedom of the individual to act or to voice a concern is considered by most Australians to be an inherent benefit of living in Western democracy': at 2. It is also noted that 'democracy as a political ideal is often taken for granted in Australian society, the commitment to freedom being an essential aspect of our lives': at 2.

[42] Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34; see also Creyke and MacMillan, *Control of Government Action*, above n7.

[43] Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34: at 3.

[44] Ibid 4.

food, clothing, shelter and medical attention is based upon 'unrealistic assumptions' and often referred to as 'positive liberty'.[45] Some liberal advocates criticise the commitment by government to social welfare policy, arguing that government regulations, taxation and revenue distribution interferes with the individual's right to compete freely in economic market activities. Sir Isaiah Berlin in 1958, for example, argued that the freedom proposed by liberal thinkers involved 'negative liberty',[46] such as freedom from constraint (including the state), freedom from laws dictating lifestyle, freedom from interference with individual decision making and freedom from restrictions on personal behaviour.

These governance choices have been thrown into high relief by a recent review of the previous government's *PCEHR* and e-health policy, commitment and progress. Due to political, economic and social changes in Australia over the last decade, including the election of a new federal government in late 2013, the in-coming administration commissioned the *Royle Review*, which focused on the merits of the new, electronic health regime and made a number of recommendations about future governance of the system.[47]

---

[45] Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34. Gaze, et al, argues that this view (negative liberty) has caused a problem for modern political theorists of the liberty tradition, 'who are currently grappling with the problem of the relationship between liberty and equality': at 4. They point out that in 'the late 19th and early 20th century, Governments began to take on more domestic policy functions': at 4. Governments regulated markets to preserve competition, 'they developed social policy by providing public education, pensions and sickness pay and healthcare, they regulated housing and working hours and conditions. 'This trend accelerated in the wake of World War 1 and the Great Depression of the 1930s': at 5. Also 'across Europe, key industries were brought into state ownership (nationalised)': at 5. In Australia, Australian Government spending on social welfare expanded dramatically during and after the war. 'Market liberalism was exiled to the margins of politics except in certain countries': at 5.

[46] See Sir Isaiah Berlin, "Two Concepts of Liberty" in *Four Essays on Liberty* (Clarendon Press, 1958) in Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34: at 4.

[47] See *Royle Review*, above n1.

III. THE ROYLE GOVERNANCE REVIEW

On 3 November 2013, the federal Health Minister, Hon Peter Dutton, commissioned a review of Australia's struggling Personally Controlled Health Records program, which had failed to attract enough doctors and consumers to participate in the project. While previous governments had laid the foundations for e-health, the adoption of the new electronic healthcare regime had not delivered the anticipated outcomes expected from its original vision and inception. The review panel membership consisted of three industry experts: Richard Royle (Chair), Steve Hambleton and Andrew Walduck.[48] No health consumer members, representing the views of this group, were appointed by the Health Minister to this committee. The completed review, which made 38 recommendations, was submitted to the Health Minister within six weeks in December 2013.

The terms of reference of the *Review* deal with (but are not limited to) *PCEHR* implementation; updating the gaps between expectations of users and what has been delivered; the governance and control systems that were applied during the development and implementation phases; key patient and clinician utility issues; the level of use of the *PCEHR* by healthcare professionals in clinical settings; the future role of the private sector in providing solutions; the policy settings required to generate private sector solutions, and the governance arrangements to set the ongoing

[48] Membership of the *Royle Review* panel include: Richard Royle (Chair) UnitingCare Health, Steve Hambleton AMA President and Andrew Walduck Chief Information Officer Australian Post.

future directions of the *PCEHR* in the context of other e-health initiatives (and timing of changes).[49]

As a consequence of the review, the 2014 federal *Budget* allocated $140.6 million to continue to support the operation of e-health and the *PCEHR* system for 12 months, while the government continues planning its response to the recommendations.[50] The current federal government refers to this phase of the *PCEHR* as the second stage of design, implementation and uptake of the system.[51]

According to the *Review* summary of findings, there is 'overwhelming support' for implementing a consistent electronic health record for all Australians.[52] However, the review accepted that a change was warranted in the approach to implementation issues, choice of strategy and the role that shared electronic health records play in the broader system of healthcare. The following sets out a list of the more pertinent *PCEHR* concerns and issues identified by the review panel:

1. Concerns with data accuracy under a patient controlled model;
2. Opt-in versus opt-out of consumers;
3. Value proposition for users until data sets are populated with clinically usable information;
4. Value proposition for users if data sets are unreliable or incomplete, and the liability and indemnity that flows from this;
5. Usability of the system at all stages of engagement;
6. Change management, in particular the lack of education and training;
7. The governance processes around the PCEHR did not adequately represent the industry and were overly bureaucratic in nature and did not effectively balance the needs of government and private sector organisations;
8. Engagement, effective consultation and buy in from a number of stakeholder groups;
9. The need for effective support for users of the system via the web;
10. Incentives and effective use of financial support to offset initial and ongoing costs of implementation for organisations and clinicians;
11. The lack of integration between current systems;

[49] *Royle Review*, above n1: at 5.

[50] Australian Government, 2014-15 federal *Budget* (2014); new federal *Budget* 2015 just released (not examined)

[51] 2014-2015 federal *Budget* (2014).

[52] See *Royle Review*, above n1: at 15.

12. The level of incentives and support for investment by software vendors;
13. Privacy and security of records remain a priority for all users and an understanding of how the privacy and security works for consumers and practitioners;
14. Development of and compliance with standards are critical for adoption of any federated system or process.[53]

In response to these perceived difficulties, the *Review* recommended that a new structure be considered dealing with matters relating to organisation, monitoring and oversight, and that ultimate decision-making be shifted to a new body, the Australian Commission for Electronic Health ('*ACeH*'), reporting directly to the Standing Council on Health *(SCoH)*.[54]

The membership of these new organisational structures effectively moves the governance focus further away from citizens and back to health professionals and industry. This is a retrograde step, in that preference will be given to private sector interests (ahead of those of citizens), such as the interests of private health insurance companies, pharmaceutical companies and IT experts gaining substantial control over individual healthcare choices, which would totally transform the original 'consumer-centric' notion of the *PCEHR* system. Locating *PCEHR* and e-health delivery (including, ultimately, welfare provision) to health industry and professional interests, without proper regulations in place, goes back on promises made by both political parties regarding implementation of fair, democratic *PCEHR* system processes and challenges the established notions of open-government and transparency of the system.

[53] *Royle Review*, above n1.

[54] *Royle Review*, above n1 Rec. 2-12.

It is acknowledged here that the *Review* makes some major contributions, such as strengthening 'networks' and *PCEHR* system inter-operability function, and that these recommendations are worthy of government consideration.[55] Nevertheless, unlike past *PCEHR* and e-health reports,[56] the *Review* seeks to preference and empowers private industry and healthcare professional providers, by committing financial incentives and public funds, to encourage commercial and professional participation.[57] These privatisation preferences ultimately diminish and reduce government public sector *PCEHR* and e-health governance control oversight, resulting in a significant reduction of 'eyes' privy to policy changes, as well as impacting on transparency mechanisms and citizen participation rights.

As previously indicated, the *Review* would begin this power 'shift' by reducing an individual to the level of 'steward' of their personal healthcare information and seeks to minimise citizen participation to that of a secondary reporting committee in the ongoing management of the *PCEHR* and e-health system. This focus 'shift' is unacceptable in light of the fact that healthcare consumers represent the majority group affected by this new electronic regime.

A. *Recommendations*

The Review emphasises the proposition that the benefits of the *PCEHR* should be realised sooner and focuses on a number of key strategies in order to achieve this

[55] *Royle Review*, above n1. Strengthening e-Health Technical and Data Foundations: at 37, for example, secure messaging (SMD), information security standards, directory services, ECLIPSE: at 72.

[56] See, for example, ALRC, *Review of Australian Privacy Law:* Discussion Paper 72 (September 2007).

[57] *Royle Review*, above n1 Even though incentives was always part of the *PCEHR* and e-health incentive scheme such as iPIPs, the *Royle Review* approach to financial and other incentives is far wider (including a broad range of peripheral health activities) and very generous in its incentive recommendation: at 44-47.

result.[58] Given the core strategies of decreasing citizen participation and increasing health industry/professional involvement, the primary recommendation made by the review is to restructure the current *PCEHR* approach to governance, dissolve *NEHTA*, effectively by-passing the Department of Health and Department of Human Services and replacing them with a new body, the Australian Commission for Electronic Health, which reports directly to the Standing Council on Health.[59] The *Review* maintains that this structure of industry actors will provide open and transparent communication on the performance of the e-health system, including oversight of the System Operator.[60]

The *Review* posits that effective and impactful governance is critical for any major investment program and that several factors are essential for building and maintaining a strong governance function. This, according to the *Review*, would include (but not be limited to) issues such as selection of trusted personnel who will represent the authority and have accountability to act, and the alignment of the governance body as an effective strategy. Empowering operating performance transparency would ensure effective decision-making and put in place appropriate framework and processes to effectively govern and coordinate investments. This strategy, it is contended, would require decision makers to act in an open, accountable way and be in regular communication with all impacted audiences.[61]

---

[58] See *Royle Review*, above n1: at 13.

[59] *Royle Review* Rec.2.

[60] Ibid 2.

[61] Ibid 20.

The *Review* provides no solid, theoretical bases for its presumptions. The recommendations it makes can be roughly divided into two groups. The first group is primarily concerned with economic, political and governance changes to the *PCEHR* system, while the second group of recommendations focuses more on practical issues, such as system governance implementation and uptake. The principal recommendation made by the review is to restructure the approach to governance and adopt a 'network' commercial and professional focus for *PCEHR* governance systems.[62]

The *Review* also recommends renaming the system from *PCEHR* (*Personally Controlled Electronic Health Records*) to *My Health Record* ('*MyHR*'), thus removing the *personally controlled* component out of the equation. This name change highlights the fact that 'the change of name will reflect more a *partnership* between the clinician and the patient.'[63] However, this observation is quite deceptive in that the *Review* states that the consumer engagement is that of a 'steward' to their records, rather than 'partnership' status.[64] This name change is rather ironic, in that the overall intent of the proposed new governance review is to take away (shift the focus) from consumers' 'ownership and control' of their personal electronic health records, towards professional and industry control. The significance of a name can be illustrated by other legislation such as the *Fair Work Act*, which some commentators argue is

[62] *Royle Review* Rec.9 - recommends dissolving *NEHTA*, disempowering and reducing the governance role of Government Departments such as Department of Health and Department of Human Services.

[63] Ibid Rec.1 - name change: at 15; see *Royle Review* recommendations in detail: at 19.

[64] *Royle Review*, above n1: at 19.

deceptive and indeed a misnomer, because workplace 'fairness' is not necessarily reflected in this Act.[65]

Additionally the *Review* recommends that the *Jurisdictional Advisory Committee* and the *Independent Advisory Council* be retained, although the *Independent Advisory Council* would now report directly to the Minister of Health and its membership would consist of industry and professional members.[66] This is a significant power shift for health professionals and industry, because the *Independent Advisory Council* would have *direct* access to the Health Minister.[67] This means that it would not be *directly* accountable to bodies such as the *Australian Commission for Electronic Health*. Other sub-committees would also be established that would report to the new *Australian Commission for Electronic Health*. These sub-committees would include a *Clinical and Technical Advisory Committee*, a *Consumer Committee* and a *Privacy and Security Committee*.[68]

Amongst the main *Review* operational changes is the recommendation that an 'opt-out', rather than an 'opt-in', model be adopted effective from the target date of 1 January 2015. However this target date has since passed and the recommendations

[65] *Fair Work Act 2009* (Cth); see Andrew Stewart, *Stewart's Guide to Employment Law* (The Federation Press, 5th ed, 2015); see also Breen Creighton and Andrew Stewart, *Labour Law* (The Federation Press, 2010).

[66] *Royle Review*, above n1 Rec. 8, Rec. 26.

[67] This direct access to the Health Minister is quite different from the original concept of the *Independent Advisory Council* operated by the *PCEHR Act* in that under this proposal there would be no intermediary reporting body (such as *NEHTA* or the System Operators) involved in the *Royle Review* proposed governance structure. The introduction of the *Council* along similar reporting lines as proposed in this thesis would, it is argued, would help restore this obvious power imbalance between professional/industry groups and citizens.

[68] See chapter 7, pp250-255 for outline of sub-committees.

made by the *Review* have not yet been implemented by the federal Coalition Government.[69] It is argued that:

> Costs associated with patient registration and the related debate around providing financial incentives to the health care industry to assist, are likely to be eliminated with the introduction of an opt-out model … For vendors, achieving a critical mass of users would help drive innovation.[70]

This would include accompanying commission technical assessment and change management for 'opt-out' process and require an annual report from the *Privacy and Security Committee* on statistics (e.g. as to who 'opted out').

Further the *Review* recommends recognition of principles of transparency, through extensive use of metrics,[71] arguing that good intentions (even if they are culturally different), plus good data (metrics), must equal good outcomes. This approach has implications for consumer healthcare data consent issues, research and secondary data use. The *Review* contends that consumers now expect initial healthcare consent to be ongoing and include an extensive range of secondary use and third party access.[72] This particular proposition — 'authorising 'free' multiple industries and research actors' access to expanded health data repositories — is argued to best advantage Australia's commercial future.[73] However, the counter argument against

[69] See *Royle Review*, above n1: at 28.

[70] *Royle Review* 55.

[71] Ibid Rec. 35.

[72] Ibid 31.

[73] Ibid. See the *Australian Health Informatics Association* (*'AHIA'*) recommendations that the legislation ensures adequate security of stored data rather than limiting the options for where data can be stored (e.g. requirement for data to be stored in Australia). The requirement to store data in Australia places limitations on potential data warehouse options such as overseas warehouses with no connection with Australia. According to *Royle Review*, this limitation 'to storing data precludes emerging and potentially more efficient and cost effective technologies such as cloud or virtualisation of servers': at 81. However, the legislation (*PCEHR Act*) that limits healthcare data storage ensures that privacy and security are paramount concerns that may not be achievable or adequately regulated overseas: at 46

'free flow' information is that without robust privacy and security mechanisms in place, personal healthcare privacy rights will be further compromised.[74] This thesis finds the latter view more compelling.

Shifting the oversight of *PCEHR* system governance away from established accountability mechanisms, such as government public sector and independent statutory bodies (e.g. the Privacy Commissioner), diminishes open government transparency and accountability, because it increases the possibility of making non-transparent decisions and effectively reduces the number of 'eyes' that contribute and protect the public interest. To claim that this new, proposed 'closed elite' system will ensure 'open and transparent communication of the performance of e-health' implementation is not supported by the nature and focus of the political agenda driving the *review* recommendations.

Consumers represent the largest, and potentially the most affected, of all stakeholder groups in the uptake of *PCEHR* systems, yet if the basic thrusts of the *Review* recommendations are accepted, it is likely that this group will be further distanced from decision-making and ultimately denied an adequate say over the future use of their personal healthcare record. The proposed establishment of a *Consumer Advisory Committee,* which constitutes one of numerous sub-committees, falls well below the anticipated type and level of consumer input this thesis argues is required by the system.

[74] Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in Andrew Kenyon and Megan Richardson, *New Dimensions in Privacy Law* (Cambridge University, 2006): at 91.

Furthermore, the *Review* says virtually nothing about individual privacy, consumer consent issues and secondary use information protection rights, framing these major concerns within a wider economic agenda.[75] It lists privacy and security as recommendation six, which suggests diminished importance. The *review* does suggest the establishment of a *Privacy and Security Advisory Committee*, which would, along with other sub-committees, report to the new Australian Commission for Electronic Health *(ACeH)*. While privacy and security numbering issues may seem 'picky' or over exaggerated (similar to the name change concerns), the reality is that privacy is being psychologically and physically relegated to a less important position and is indicative of the 'focus shift', away from promised *consumer-centric* control and privacy concerns, and towards multiple third parties 'sharing' personal healthcare information.

The *Review* also recommends establishing a regulatory body that monitors and ensures compliance against e-health standards that are set and maintained by the *ACeH*. The spirit of this proposal represents a positive and important move, to ensure harmonised, national e-health standards. However, the down-side to this recommendation is that it fails to provide any real detail explaining how this regulatory body would be constituted and function, such as how membership would be determined or what its responsibilities would be.[76] Given that this is, arguably, a very important governance mechanism process; the lack of any significant detail is disappointing compared with the *Concepts of Operations: Relating to the Introduction of*

[75] See *Royle Review*, above n1.

[76] Ibid 16, 26.

a Personally Controlled Electronic Health Record (*Concepts of Operations*),[77] which at least attempted to provide operational detail regarding its recommendations.[78]

The *Review* makes no significant recommendations about consumer complaint mechanisms and does not include accountability to consumers for their privacy, in the list of effective and impactful governance recommendations. In fact, the *review*, if accepted, further strengthens the requirement that there be an immediate update of the *MyHR* strategy to actively enable 'decentralisation' and 'networking' of information across multiple data repositories to occur, with information being linked using the *HI*. It also recommended that by 1 January 2015, Medicare item number requirements for health assessments, comprehensive assessments, mental health care plans, medication management reviews and chronic disease planning items require a copy of the information to be uploaded to the *MyHR*. However, as noted earlier, this 2015 date has now passed without the implementation of these recommendations. This Medicare item number covers most areas of healthcare delivery, and despite the potential sensitivity of information (such as mental health care plans) and obvious lack of voluntary consumer acceptance of the impact this will have on individual healthcare privacy, this information would automatically be added to every person's *MyHR*.

There is no argument in this thesis against the *Review* proposition that the approach to the *PCEHR* system needs to be reconsidered in light of advancing

[77] Australian Government, National Electronic Health Transition Authority (*NEHTA*), *Concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* (September 2011).

[78] Ibid.

economic and social developments. Indeed, the upgrade to strengthen e-health technical and data foundations, such as secure messaging and the creation of an 'e-health ecosystem', are generally sound and sensible propositions. Nevertheless, this proposition could be realised by using a fairer and more democratically inclusive way to change the system, and the governance model in the *Review* ought to be modified and adopted according to principles that promote adequate, individual privacy protection and democratic ideals. This new proposed governance overview, outlined in chapter 7, does not displace the necessity for the involvement of commercial expertise and professional healthcare input, but it does rank and *prioritise* this level of interest below those of the general public and democratic processes.

It was anticipated, by the *Concepts of Operations* that a multi-layered approach would adequately safeguard the *PCEHR* system and incorporate both technical and non-technical controls, including accurate authentication, audit trails, proactive monitoring, rigorous security and requirements that healthcare providers and organisations comply with specific *PCEHR* system business rules and relevant legislation.[79] This commitment to privacy resulted in the adoption of technical advancement outcomes — *Privacy by Design* and technical self-regulation 'evolution' — to further ensure strong, privacy and security protection measures. [80]

---

[79] NEHTA, *Concepts of Operation*, above n77: at 17.

[80] Ibid; NEHTA, *e-Health Architecture, Interoperability and Standards* http://www.nehta.gov.au/connecting-australia/ehealth-architecture (viewed on 15/4/2013). This document identifies three key Architectural paradigms: 1) National e-Health Architecture (sector-wide), which provides 'both capability and solutions views for e-health in Australia; 2) E-Health interoperability specifications, national infrastructure solutions and frameworks development; 3) NEHTA, Enterprise Architecture, which utilises traditional Enterprise Architecture approaches ensuring strategically aligned, consistent deliverables and outcomes. 'The e-health Interoperability Framework provides a shared language for defining business context for e-health systems, designing e-health solutions and standards-based conformance processes. The aim is to provide an increasing

Privacy by Design maintains that in order to adequately protect electronic healthcare privacy rights, there must be actively 'embedded' privacy and well-designed security systems implemented early (upfront) into new health information technology designs (e.g. hardware, programs, software), and business practices, to facilitate 'gold standards' in personal health information sharing and individual privacy protection in the information era.[81] This design concept is based upon a proactive approach, with an emphasis on 'positive-sum and win-win' outcomes for privacy protection, which encompass seven foundational principles such as: proactive not reactive; privacy as a default setting; privacy embedded into design; full functionality; positive-sum not zero-sum; end-to-end security: full life-style protection, and visibility and transparency: keep it open and respect for user privacy: keep it user-centric.[82]

Commitment to *Privacy by Design* by the previous federal government acknowledges that adequate system design (e.g. such as 'default' options) will take time and effort to build the necessary framework for protecting consumer privacy in

level of semantic interoperability both between humans involved in designing and building systems and between e-health systems': at 1-4.

[81] See Ann Cavoukian, Information and Privacy Commissioner Ontario, Canada, *Embedding Privacy into Health Information Technology: An Absolute Must* (June 2010); see also Ann Cavoukian, Information and Privacy Commissioner Ontario, Canada, 'Privacy by Design: Strong Privacy Protection Now and Well into the Future' (Paper Presented at 33rd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 29 October 2010); See Ann Ohlden, 'Landmark Resolution Passed to Preserve the Future of Privacy, Adoption of Privacy by Design as an International Standard' (Paper Presented at International Data Protection and Privacy Commissioners, Jerusalem, 29 October 2010);

[82] See Ann Cavoukian, *Embedding Privacy into Healthcare Information Technology*: *An Absolute Must*, above n81. The seven *Privacy by Design* Foundational Principles are: 1. Proactive not Reactive; Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded into Design; 4. Full Functionality; Postive-Sum, not Zero-Sum; 5. End-to-End Security: Full Lifecycle protection; 6. Visibility and Transparency: Keep it Open; and 7. Respect for User Privacy: Keep it User-Centric: in Information and Privacy Commissioner of Ontario, Canada, *Privacy by Design* (Paper presented at 33rd International Conference of Data Protection and Privacy Commissioners Report, 30 October 2011).

an era of rapid global change.[83] This implies careful consideration of any new technology, and promotes the idea that rather than rushing to adopt innovative, novel and untested technology, even in a competitive market environment, all options must be carefully considered in order to secure 'long-term', robust privacy and security protection design and governance outcomes.[84]

IV. 'CONCEPTS OF OPERATIONS' GOVERNANCE VISION

As a result of *EPR* research and inclusive community consultation over more than a decade by government, which clearly indicated ongoing public anxiety about *PCEHR* individual privacy rights, the long-term plan adopted by various federal Governments (both when elected and while in opposition) for its development and implementation favoured a 'consumer-centric', 'opt-in' *EPR* consent model, whereby healthcare consumers voluntarily enrolled and participated in the *PCEHR* system. Previous governments envisaged that the 'trilogy' combination of robust legislation, governance and technical reform measures would continue to 'balance' the needs and interests of individuals and business in the new e-health regime. This would ensure

[83] See Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, *Submission of the Information & Privacy Commissioner, Response to the FTC Framework for Protecting Consumer Privacy in an Era of Rapid Change* (21 January 2011).

[84] Ann Cavourkian, *Submission of the Information and Privacy Commissioner, Response to the FCT Framework for Protecting Consumer Privacy in an Era of Rapid Change*, above n83; Ann Cavourkian, *Reject Unlawful Surveillance – Stand Up for Privacy and Freedom by Design* (28 February 2014) The Electronic Surveillance State Canadian International Council; see also Ann Cavourkian, *Privacy by Design in the Age of Big Data* (12 June 2014) DMM Analytics; see also Eugeny Morozov, "The Real Privacy Problem", above 4; see also Tal Zarsky, "Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion" (2003) 5 *Yale Journal of Law and Technology.*

stakeholder and public trust and confidence, as well as persuade voluntary uptake of the *PCEHR* by consumer and healthcare providers.[85]

The earlier proposed *PCEHR* system operation framework, largely contributed to by the ALRC report on privacy in Australia and physically manifested by *NEHTA*, reflected a theoretical, conceptual model based upon participatory institutional governance, placing the healthcare consumer at the forefront of 'control' of their electronic healthcare record.[86] However, the reality of just how much consumer 'control' should be exercised was (and still is) a hotly debated issue by consumer advocates, health industry stakeholders and healthcare professional groups.[87]

The Australian Medical Association ('*AMA*'), for example, has remained particularly vocal and sceptical regarding 'consumer-centric' *PCEHR* 'control', arguing the merits of consumer capacity to reliably and accurately manage their own healthcare information.[88] The *AMA* also vehemently criticised the proposed

[85] See NEHTA, *Concepts of Operation*, above n77: at 8; see also chapter 2, pp38-67 for discussion on Government *PCEHR* and e-health policy.

[86] Consumer Health Forum (*CHF*), "Consumers have told Consumer Advisory Committee that they want to actively participate in the management of their records, rather than passively enable providers to enter information" quoted in *Royle Review*, above n1: at 30.

[87] See, for example, *Royle Review*, above n1: at 53; Paul Smith, 'Non-Medical E-Health Curators Risky' *Australian Doctor* (Australia), 17 June 2011, 3; David Braue, 'E-Record Support Comes at a Price' *Medical Observer* (Australia), June 2010, 9; Paul Smith, 'GPs to be E-Record Guardians' *Australian Doctor* (Australia), 18 March 2011, 1.

[88] Australian Medical Association (*AMA*), 'Personal Control versus Clinical Need for Complete Unedited Records' (Press Release by *AMA*, 26 November 2013). It was reported that "We support people taking greater responsibility for their own health and the *PCEHR* has the potential to assist with this, but patient control should not mean that the *PCEHR* cannot be relied upon as a trusted source of key clinical information" quoted in *Royle Review*, above n1: at 30.

'subordinate' curator/guardian role of doctors in the scheme, decrying the increased workload and lack of monetary compensation associated with its adoption.[89]

As a consequence of pressure on government from professional and business interest lobby groups, the final *Concept of Operations* report was significantly different from the original *consumer-centric* model first proposed by NEHTA, because it contains multiple compromises and reversal of *PCEHR* consumer control promises made by various governments over the years. Nevertheless, it is accurate to say that the final *Concept of Operations* does contain many positive, innovative and affirmative privacy protection measures, such as robust systems audits, 'opt-in' consent mechanisms, and security update system requirements and in certain circumstances, consumer controls that can limit *PCEHR* access.[90] In addition, the report included a firm commitment by government to further implement technical privacy and security protective measures such as *Privacy by Design,* discussed earlier in the chapter.[91]

Prior to the change of federal government in Australia in late 2013, the previous Australian Labor government[92] made significant and substantial progress in *PCEHR* system development, architecture, interoperability measures and privacy protection design, by adopting a systematic approach to its implementation.[93] As a starting point, taking what government considered being the most important ALRC

[89] *AMA*, 'Personal Control versus Clinical Need' (Press Release by *AMA*, 26 November); see Paul Smith, 'Patients to Censor Own E-Health Records' *Australian Doctor* (Australia), 22 April 2011, 2.

[90] See *NEHTA*, *Concepts of Operations,* above n77. [Where the original Government vision of consumer control is greatly modified in this final report].

[91] See chapter 3: at pp81-97; chapter 4: at pp99-120.

[92] The previous federal Government was the Labor Government (2006-2013). The current Australian Government (2013 onwards) is the Coalition Liberal-National Government.

[93] See *NEHTA*, *Concepts of Operations*, above n77.

recommendations, it conceived and designed the system architecture and introduced new legislation and regulations to progressively support the new system. This process culminated, some critics argue, prematurely, in the official launch of the *PCEHR* consumer enrolment program in July 2012.[94]

Nonetheless, despite time, effort, public inclusion consultations,[95] business support, industry and professional partnership agreements, general practitioner incentive programs and the ongoing financial commitment from federal government, there has been disappointing progress in the new *PCEHR* system reaching targets of expected voluntary consumer and healthcare provider uptake.[96] Similarly, there has also been a noticeable lack of positive, identifiable *PCEHR* and e-health systems governance processes and outcomes in place. Thus, the current situation is that

---

[94] See Suzanne Williams, 'GP Uploads First-Ever E-Health Record' *Australian Doctors* (Australia), 14 September 2012, 5; Rhonda Jolly, 'The e-Health Revolution – Easier Said Than Done' (Research Paper No. 3, Parliamentary Library, 17 November 2011). [Where it was noted that 'the National Health and Hospitals Reform Commission supported the introduction of personal electronic health records, recommending that they be in place by 2012 (NHHRC, *A Healthier Future for all Australian: Final Report* (December 2008)]. It was recognised that this date represented an ambitious target requiring considerable commitment by Government at all levels, and some commentators labelled it almost impossible to achieve': at 40; see also Karen Dearne, 'E-health Shock for Roxon', *The Australian*, (Australia), 29 July 2009, 51.

[95] See Rhonda Jolly, 'The E-Health Revolution - Easier Said than Done', above n94. Jolly noted that consultation and feedback was available via NEHTA's, *Draft Concepts of Operations Relating to the Introduction of a Personally Controlled Electronic Health Record System* (April 2011). Feedback on the *Draft Concept of Operations* closed on 7 June 2011. 'Consumers, medical providers and IT experts expressed dissatisfaction with the *Draft Concept of Operations* plan. However, the Government noted that consumer (and other groups) had been consulted in the development of the *National E-Health Strategy* and the design and privacy framework for the Healthcare identifiers Service': at 34. In September 2011, a revised *Concepts of Operations* paper was released. The updated *Concepts of Operation,* above n77. This report noted the comments on proposals received. This had been reviewed independently by Deloitte and between the Departments of Health and Human Services and NEHTA.

[96] NHHRC, *A Healthier Future for all Australians: Final Report,* above n94. 'The Commission advocated a 'middle out' approach to e-health to give government national responsibility to create a common set of technical goals and underpinning standards to accelerate and adequately resource the *National E-Health Strategy*.' See Rhonda Jolly, 'Easier Said than Done', above n94. According to Jolly, as one analyst phrased it, the approach was an attempt to develop a system which could 'avoid the opposite extremes of an industry free-for-all and bureaucracy's dead hand': 35; Karen Dearne, 'E-Health Could be a Reality by 2012', *The Australian* (Australia), 28 July 2009

despite the plethora of new legislation and other governance measures in this area, the current system falls short of addressing the main privacy protection concerns identified in earlier reports, in a number of significant ways.

Key components of 'shared' electronic healthcare records include proper authentication systems and the mandatory adoption of *HI* numbers for consumers and healthcare providers. This requirement is implemented in the *Healthcare Identifiers Act 2010* (Cth).[97] In conjunction with the *Healthcare Identifiers Act*,[98] the *PCEHR Act*[99] set out the proposed governance arrangements for the *PCEHR* system. The *PCEHR Act* establishes the legal and regulatory framework under which the *PCEHR* system operates, as well as the privacy regime, which governs the system and operates in tandem with federal, state and territory privacy laws.[100]

Balancing the needs of consumers, healthcare providers and industry was not without its complications, however, despite these complications with feedback sufficient time was allowed for public participation. During the earlier *HI* feedback process, consumer advocate groups, and some State Privacy Commissioners,[101]

---

[97] *Healthcare Identifiers Act 2010* (Cth).

[98] Australian Government, Australian Health Ministers' Advisory Council, *Healthcare Identifiers and Privacy: Discussion Paper on Proposals for Legislative Support* (July 2009); Australian Government, *First Stage Response to the ALRC Recommendations* (August 2009); see also chapter 5, pp163-182 for discussion of legislative response to PCEHR and e-health systems.

[99] *Personally Controlled Electronic Health Record Act 2012* (Cth).

[100] National Health and Hospitals Reform Commission (NHHRC), *A Healthier Future for all Australians: Final Report*, above n94. The Commission's analysis echoed 'long-standing' themes of the need to coordinate and harmonise legislative response to e-health initiatives. Despite some e-health initiatives at federal, state and territory levels, lack of connectivity across jurisdictions and settings in healthcare meant that information sharing within the national health system was at 'best fragmented, and at the worst, non-existent' in Rhonda Jolly, 'Easier Said than Done', above n94: at 29.

[101] See, for example, Office of the Victorian Privacy Commissioner, *Submission to the Senate Standing Committee on Legal and Constitutional Affairs on Healthcare Identifiers Legislation* (9 July 2012); See CSC Healthcare Research Group, *A Rising Tide of Expectations* (July 2010), CSC (CSC is not an abbreviation of the name) [notes Australian consumers' views on electronic health records – a necessary ingredient

expressed concerns about the possibility of extended commercial use of the *HI* number.[102] As a consequence of these concerns, legal assurance was given that the *HI* number allocated to citizens would not be available for use by private organisations that did not provide direct healthcare services to the public.[103] However, the *Review* challenges the legally protected use of the *HI* number and recommends that the legislation be changed to extend its adoption, to include wider and peripheral commercial purposes.[104] This recommendation goes against the previous understanding, assurances and promises that the Australian Government gave to the general public about the intended use and protection of *HI* numbers.[105]

The *PCEHR Act* introduced a range of mechanisms to provide transparency and scrutiny of the *PCEHR* system's operation, including the review of decisions by the System Operator, annual reports by the System Operator, reports by the OAIC and reviews of legislation. It also established two new advisory bodies, a *Jurisdictional Advisory Committee* and *Independent Advisory Council*.[106] The *Jurisdictional Advisory Committee* would provide advice to the System Operator on matters relating to the

---

in healthcare reform, noting that 'most Australians see themselves as being in control of their healthcare' and that this remains important to the success of health reform in Australia]: at 7.

[102] See Rhonda Jolly, 'The e-Health Revolution: Easier Said than Done', above n94: at 30; see Danuta Mendelson, "Healthcare Identifiers Legislation: A Whiff of Fourberie" (May 2010) 17(5) *Journal of Law and Medicine* 660; see also Office of the Australian Privacy Commissioner, *Submission on the Healthcare Identifiers and Privacy: Discussion Paper on Proposal for Legislative Support* (2009); Australian Privacy Foundation, *Submission to Healthcare Identifiers and Privacy: Discussion Paper on Proposals for Legislative Support* (August 2009); COAG, Australian Health Ministers' Conference, *Joint Communique* (Media Release, 13 November 2009).

[103] This provision is subject to exemptions. This assurance that the HI consumer number would not be used for other commercial purposes included those organisations that did not directly deliver a healthcare service (doctors, allied healthcare, hospitals). See *Healthcare Identifiers Act 2010* (Cth).

[104] *Royle Review*, above n1: at 38-40.

[105] See Rhonda Jolly, 'The e-Health Revolution: Easier Said than Done', above n94: at 35.

[106] See chapter 5, pp174-181 for discussion of Commonwealth legislation and the establishment of the Jurisdictional Committee and Advisory Council.

interests of the Commonwealth, states and territories in the *PCEHR* system. The *Independent Advisory Council* would provide advice to the System Operator and NEHTA on the operation and participation in the *PCEHR* system, together with clinical, privacy and security matters relating to the *PCEHR* system's operations.

Despite good intentions behind the establishment of these two advisory bodies, a number of management issues emerged relating to the operation of the *PCEHR* system and in particular, the decision-making activities of the System Operator and NEHTA, resulting in an impasse between the *Independent Advisory Council*, medical practitioner members and NEHTA. This resulted in all of the medical practitioner representatives resigning from the Council.[107]

V. CONSTRUCTING MODERN ERA GOVERNANCE

The adoption of public sector, economic, rationalist management approaches by the Australian Government, in line with most Western capitalist countries,[108] has resulted in a growing 'conflict of interest' gap between business propositions, based upon principles such as 'commerce in confidence', productivity and efficiency values, and established public sector traditional values such as open government, transparency and accountability. Generally, Australian Governments have managed to 'balance' the interests of public and private demands, nevertheless expanding global

[107] See, for example, Steve Hambleton, 'To All E-Health Questions the Answer Seems to be 'No'' *Australian Doctor* (Australia), 8 June 2012, 22; Paul Smith, 'GPs to be E-Record Guardians' *Australian Doctor* (Australia), 18 March 2011, 1; Paul Smith, 'Non-Medical E-Health Curators Risky' *Australian Doctor* (Australia), 17 June 2011, 3; David Braue, 'E-Record Support Comes at a Price' *Medical Observer* (Australia), October 2010, 9; Michael East, 'A Record Revolution' *Australian Doctor*, (Australia), 24 June 2011, 45.

[108] See, for example, Robert Locke and J C Spender, *Confronting Managerialism* (Zed Books, 2011); Peter Jackson, Michelle Lowe, Daniel Miller and Frank Mort (eds), *Commercial Cultures* (Berg, 2000).

marketplace pressures and expanding technology, threaten to diminish the rights of citizens, and compromise elected governments.[109]

Governance was once synonymous with central government (or the 'state'), but more recent usage of the term involves something quite different — the production of collective outcomes (in the context of public problems) that is not controlled by a centralised authority. The decision-making power of public administrators, or formal government, diffuses outwards to be exercised by industry groups, interest groups, non-government organisations, private businesses, research institutes, professions and academics; while inside government, agencies with different objectives and goals compete and are often balanced off against each other.[110]

The purpose of governance is to ensure strategic oversight measures, operational management and regulatory oversight functions of the system. However, governance can also be defined narrowly as 'the act or manner of governing, the office of function of governing, archaic sway control.'[111] This view of governance implies both the physical and psychological act itself of governing, plus recognition and implementation of the values and manner in which governing function norms are determined in society. For the purpose of the governance reforms recommended in this thesis, the concept of governance has a far broader meaning than just the manifestation of day-to-day management instruments, such as rules, regulations, obligations, compliance and dispute mechanisms which are adopted by government

[109] See Jack Balkin, 'Information Power: The Information Society from an Antihumanist Perspective' in Subramanian, and Katz, *The Global Flow of Information*, above n9: at 232; Kenyon and Richardson, *New Dimensions in Privacy Law* (Cambridge University Press, 2006).

[110] Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 140-141.

[111] The word 'Governance' defined in Oxford Dictionary.

bodies or other institutional and economic interests. Governance, as viewed in this broader light, encompasses core social values. It includes ethical principles and cultural norms and expectations that underpin democratic social contracts between citizens and states, encompassing principles such as transparency, open government, distributive justice, accountability, efficiency, efficacy and productivity.

As previously noted, the governance function represents a key factor for promoting both *PCEHR* consumer and healthcare provider confidence and uptake of the new electronic health regime, as well as providing further assurances to citizens as to ongoing, adequate, individual healthcare privacy protection. A strong commitment to *PCEHR* governance was made by the previous Australian Government, which resulted in the enactment of the *PCEHR Act* as an important first stage government response, setting out governance requirements based upon ALRC recommendations relating to e-health privacy protection and governance.[112]

As a result of rapidly increasing, modern-day, global economic pressures on governments – such as the need to sustain worldwide, competitive economic growth, marketplace deregulation and free trade agreements – all areas of traditional administrative government operation are now subject to intense scrutiny by many different industry and professional actors wishing to participate in decision-making activities. Questions now surface as to traditional public sector authority, regulatory and governance roles in the new global networked system. Unlike the hierarchy of

[112] See *Personally Controlled Electronic Health Records Act 2012* (Cth); see also ALRC, Discussion Paper 72, above n56; see also chapter 3, pp81-97; chapter 4, pp99-120.

nation-state governance, these new initiatives often rely on 'heterarchic' or 'network'-like relationships.

These new forms of political regulation operate above and beyond the nation-state, in order to re-establish the political order and circumscribe economic rationality by new means of democratic control. Consequently, with intensified engagement of private actors and social movements, and the growing activities of international institutions, a new form of '*trans*-national regulation is emerging — global governance, the definition and implementation of standards of behaviour with global reach.'[113] It is not only public actors, such as national governments and international governmental institutions (e.g. UN, ILO, OECD, WHO) that are contributing to this new-world order.[114] These global governance initiatives also often present themselves as public-private or public-private partnerships of multi-stakeholder interests, which have been described as a 'new form of governance with the potential to bridge multilateral norms and local action by drawing on a diverse number of actors in civil society, government and business.'[115]

Traditional approaches to governance rely on national governance systems with proper execution of formal rules (hard law), through the legal and administrative

[113] See Scherer and Palazzo, "The New Political Role of Business in a Globalised World", above n13: at 909.

[114] See Belinda Bennett, 'Globalising Rights? Constructing Health Rights in a Shrinking World' in Belinda Bennett, Terry Carney and Isabel Karpin (eds), *Brave New World of Health* (The Federation Press, 2008): at 8; see also Terry Carney, 'Where Now Australia's Welfare State' (2013) iv *Diritto Pubblico Comparato ed Europeo* [Journal of Comparative and European Public Law] 1353-1370.

[115] See Karl Backstarnd, "Multi-stakeholder Partnerships for Sustainable Development: Rethinking Legitimacy, Accountability and Efficiency" (2006) 16 *European Environment* 291; see Rebekah Gay, "Mainstreaming Wellbeing: An Impact Assessment for the Right to Health" (6 June 2008) 13 *Australian Journal of Human Rights* 33; John Braithwaite, "Responsive Regulation and Developing Economies" (Published by Elsevier on 21 April 2005) (online)) www.elsevier.com/locate/worlddev (viewed on 17/8/2010).

system (sanctions). Non-political actors are required to 'play the game' according to the rules, through mechanisms of enforcement in a hierarchical system of 'command and control'.[116] Even under the auspices of 'self-regulation', it is assumed that they operate in the 'shadow of hierarchy', meaning there is the conceivable threat that stricter regulations will be enacted, unless the potentially deviant business adapts their behaviour to expectations of the legislator.[117]

The global governance problem is well addressed in international relations and political science scholarship, where the concrete design of private-public policy networks, in the regulation of global issues, is discussed. It is argued that, within the context of the global regulation and production of public goods, neither nation-state agencies nor international institutions have the knowledge and capacity to resolve the issues.[118] Rather than just focusing on state actors and international institutions, such as the United Nations Declaration of Human Rights, World Trade Organisation and International Labour Organisation[119] alone, political theorists acknowledge the role that non-government organisations ('*NGO*') and private business firms play in global (and arguably national) governance.[120]

---

[116] See John Braithwaite, *Regulatory Capitalism,* above n28.

[117] T Shillemans, "Accountability in the Shadow of Hierarchy: The Horizontal Accountability of Agencies" (2008) 8 *Public Organisation Review* 175.

[118] John Braithwaite and P Drahos, *Global Business Regulation* (Cambridge University Press, 2000).

[119] See United Nations, *Universal Declaration of Human Rights* of 1948, General Agreement on Tariff and Trade (GATT), established in 1947, and later in 1994 the World Trade Organisation (WTO); *International Covenant on Civil and Political Rights* in force 1966; *International Covenant on Economic, Social and Cultural Rights* in force 1976; *International Labour Organisation*, a body established after World War 1 (1916) and of which Australia was a founder member. The ILO is a tripartite body whose parliament, the International Labour Conference, is comprised of representatives of employers, workers, unions and government from each member state. Merely by belonging to the ILO, Australia is committed to observe the core principles on which the ILO operates.

[120] See Scherer and Palazzo, "The New Political Role of Business in a Globalised World", above n13.

As earlier mentioned, the growing engagement of business firms in public policy leads to concerns of a democratic deficit; in other words those who are democratically elected (government) to regulate have less power to do so, while those who are engaged in self-regulation (private corporations) have no democratic mandate for this engagement and cannot be held accountable by a civil polity. From a classical, liberal point of view, corporations are private, not political actors. Deliberative democracy theory, as outlined earlier, is often suggested as an alternative model, which it is argued 'seems better equipped to deal with the post-national constellation and to address the democratic deficit.'[121]

A. *Hard or Soft Law Approach?*

In a complex economic society, such as Australia, there is a move away from a 'hard law' to 'soft law' regulatory or governance approach.[122] Governments have generally responded to regulatory challenges by way of delegated legislation (e.g. regulations) or other quasi-legislation (such as standards or guideline declarations), which devolve the power of day-to-day management to subordinate bodies such as independent commissions, specialist committees, authorities and non-government organisations.

[121] Scherer and Palazzo, "The New Political Role of Business", above n13: at 907 [a review of a new perspective on CSR and its Implications for the firm, governance and democracy].

[122] See Penelope Simons and Audrey Macklin, 'The Governance Gap: Multistakeholders and Intergovernmental Initiatives' in Simons and Macklin, et al, *The Governance Gap,* above n11: at 79; see also Greg Weeks, 'The Use and Enforcement of Soft Law by Australian Public Authorities' (Paper Presented to the Practice and Theory of Soft Law Academic Symposium, Peking University Soft Law Centre, 9 July 2011); See Penelope Simons 'Private Law Beyond the State: Harder Than Hard Law' in Simons and Macklin, *The Governance Gap*, above n11: at 88; Julia Black, 'Critical Reflections on Regulation,' above n22; see also, Roger Cotterrell, *The Politics of Jurisprudence* (Butterworths, 1989) 83.

This allows for greater self-regulating power and control in determining their preferred governance process.[123]

This new form of governance establishes a new institutional context with private actors in a regulatory role; it also relies on a different form of regulation, the so-called 'soft law' approach that operates without a governmental power to enforce rules and to sanction deviate behaviour. As a consequence, self-regulation is becoming a key issue in this debate, thus favouring a 'soft law' approach to issues such as industry and professional compliance measures.[124]

Another related discourse promulgated by scholars draws on legal pluralism, as well as new governance scholarship.[125] This discourse contends that certain *trans*-national, self-regulatory initiatives together have created a 'working networked system of governance that is substantially greater than its parts.'[126] Legal pluralist scholars dispute the positivist hegemony of the state, in the development and enforcement of law, and put forward 'a poly-centric or poly-morphic concept of law', questioning the distinction between legal rules enacted by the state and norms created by non-state actors.[127] From a legal pluralist view, the state is only one source of law and consequently, state-made law is only one form of law.

---

[123] See Greg Weeks, 'The Use and Enforcement of Soft Law by Australian Public Authorities', above n122.

[124] Ibid.

[125] See Larry Cata Backer, 'Governance without Government: An Overview' in G Handl, J Zekoll and P Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalisation* (Martin Nihhoff Publisher, 2012): at 87, 118.

[126] Penelope Simons, 'Private Law Beyond the State: Harder than Hard Law?' in Simons and Macklin, *The Governance Gap*, above n122: at 88.

[127] Simons and Macklin, *The Governance Gap*, above n122.

Some theorists contend that corporate codes and even multi-stake holders, Corporate Social Responsibility ('*CSR*') initiatives can be seen as private/public/private legal orders that articulate, but do not depend upon, state-based law and are normatively equivalent to state-created law.[128] It is argued that the decline in governance capability of nation-states is partly compensated by the emergence of new forms of global governance, above and beyond the state. Scherer and Palazzo contend that, in this new global governance age, public issues once covered by nation-state governance may now fall under the discretion and responsibility of corporate managers.[129]

B. *New Reflexive and Network Governance Models*

What is now being proposed by some commentators is a 'new reflexive governance' regime, which may or may not include the government as a regulator. In fact, the very foundation of state sovereignty and the future role of government in regulating corporate and business interests are under threat by dominant forces, such as market liberalism, corporatism, multinational corporate enterprise ('*MNE*'s) interests, pluralist and neo-pluralist transformation politics and globalisation. The main consideration of such 'reflexive' and 'network' governance models is the recognition, integration and transfer of power to other actors, beside traditional government and its agents, as political and social change actors in a 'post national' constellation era. New reflexive models identifies sophisticated, complex, 'networking' systems

[128] See Scherer and Palazzo, "The New Political Role of Business in a Globalised World", above 13: at 1; G Teubner, "Self-Constitutionalizing TNCs? On the Linkage of 'Private' and 'Public' Corporate Codes of Conduct" (2011) 18 *Indiana Journal of Global Legal Studies* 617; see generally John Farrar, *Corporate Governance* (Oxford University Press, 2005) 52.

[129] See Scherer and Palazzo, "The New Political Role of Business in a Globalised World", above n13.

technology that includes, not just traditional hierarchical actors (such as government), but also vertical, multiple, economic actors contributing different interests and skills, as the new source of legitimacy in a global economy.[130]

Thus, the theory of 'reflexive law' falls under the broad umbrella of new management governance. It is premised on the concept of law being one of many 'autopoietic' societal subsystems — self-referencing and self-reproducing.[131] Drawing on Systems Theory and the work of Niklas Luhmann, law is conceived as one of many normative subsystems, such as religion, and like other normative systems; law is operationally or normatively closed, yet cognitively open.[132] Substantive law is, therefore, unable to effectively influence behaviour within the various social subsystems, since each subsystem will process law according to its normative structure.[133] According to Teubner, the solution to the deficiencies of substantive regulation lie in 'reflexive law', which restricts legal performance to more indirect, abstract forms of social control.[134] Like 'reflexive law', 'responsive law', developed by

---

[130] See Simons and Macklin, *The Governance Gap,* above n11 cites G Teubner: at 13; see also L C Backer, 'Governance without Government: An Overview' in Handl, Zekoll and Zumbansen, *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization*, above n125.

[131] G Teubner, 'Introduction to Autopoietic Law' in G Teubner (ed), *Autopoietic: A New Approach to Law and Society* (Walter de Gruyter, 1988): at 1-2; see Julia Black, 'Proceduralising Regulation: Part 1' (2000) 20:4 *Oxford Journal of Legal Studies* 597; see also L C Backer, "Rights and Accountability in Development ('Raid') v Das Air and Global Witness v Afrimex: Small Steps Towards an Autonomous Transnational Legal System for the Regulation of Multinational Corporations" (2009) 10 *Melbourne Journal of International Law* 258.

[132] See Niklas Luhmann, *Social Systems* (books.google.com. 1995); Niklas Luhmann, 'Familiarity, Confidence, Trust: Problems and Alternatives' in Gambetto Diego (ed), *Trust: Making and Breaking Cooperative Relations* (Oxford University Press, 2000): at 94-107.

[133] See Humberto Mariotti, 'Autopoiesis, Culture, and Society' (online) http://www.oikos.org/mariotti.htm (viewed on 15/9/2014).

[134] See G Teubner, 'Justification – Concepts, Aspects, Limits, Solutions' in G Teubner (ed), *Juridification of Social Spheres* (Walter de Gruyter, 1987) cited in Simons and Macklin, *The Governance Gap*, above n11: at 13-14.

Ian Ayers and John Braithwaite, falls within the concept of new governance or 'decentred' forms of regulation.[135]

New theories of governance reflect the complex direction of an advanced post-industrial society, within which there is no longer any single dominant point of societal leverage. Civil regulation is one kind of activity where some of the traditional functions of government seem to have been usurped by non-governmental actors.[136] Further social change is driven, largely, by international influences, examples and pressure. Pluralist agents stress the importance of 'networks', or policy communities, in the new governance age.

'Networks' can involve actors from different interest groups, the professions, social media, and non-governmental organisations — even from other countries.[137] As previously noted, 'networked' governance is pluralistic in the sense that it involves many different actors in the production of collective outcomes. Theorists of 'network' governance assign less significance to the formal moments of legislation and executive decision that pluralists once highlighted. This form of governance also differs from corporatism, because much of the action does not occur in peak, level negotiations between a small set of major players — it is more decentralised than that. 'Networks' are generally organised horizontally, rather than hierarchically, which follows from the presumption that there is no sovereign power within a network.[138]

---

[135] See Ian Ayers and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992) 35.

[136] See John Braithwaite, "The Essence of Responsive Regulation" (2011) 44 *UBC Law Review* 476; see Ian Ayers and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate,* above n135.

[137] See chapter 3, pp78-97 for discussion on 'network' technology advances.

[138] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10: at 142.

The rise of 'network' governance poses some major questions for the theory of the liberal, democratic state: most notably, whether it is still really democratic, or indeed still a state in the traditional sense. Electoral democracy means accountability of government to the voters. Hence, the basic problem for the state is how to convert private interests into some form of public benefit. Market liberals may accept democracy, but they generally believe that any sort of politics is full of deficiencies and problems, compared with 'virtuous' markets. The basic agenda of market liberals is clear enough: shrink the role of government so that it performs no more than the essential functions described above.

The development in the organisation of institutions and policy making in many societies, such as Australia, can be interpreted in light of contemporary pluralism. This model emphasises the degree to which models of collective decision in plural societies now feature governance, rather than government. The *Royle Review*, however, simultaneously reduces the official overview role of government (and by extension citizens) participation and extends the importance and role of economic and professional actors — highlighting economic imperatives that recognise 'effective and impactful governance is critical for any major investment program.'[139]

This model argues that strong governance alignment must consider an effective economic strategy, which will realise the economic, marketplace, profit-generating potential of the *PCEHR* system. In order to achieve this economic competitive outcome, governance control is extended to non-government actors and relocated

[139] *Royle Review*, above n1: at 20.

beyond traditional government representatives; thus potentially favouring healthcare professionals and the private health industry in elite decision-making processes , and elevating IT vendor groups as prominent decision leaders.[140] Citizens are reduced to the position of consumer, a receiver of goods and services.

Although the *Review* lacks any significant theoretical grounding it is, nevertheless, best interpreted from an elite market, liberal, neo-pluralistic, 'network' perspective. Reconceptualising certain propositions advanced in the *Review PCEHR* governance structure and introducing a *Council* into the equation, as detailed in chapter 7 would help to redress the balance, by better realising the promotion of representative democracy. However, emphasis must be placed upon the notion that the *Council* is a significant, component of the overall, healthcare privacy solution. Further, it is noted that its introduction does not mitigate what democratic elected governments are morally required to do;[141] that is, provide strong, transparent and accountable leadership and retain oversight of the *PCEHR* and e-health system, by developing adequate, individual healthcare privacy protection regulations and governance processes for the benefit of citizens.

Without a clear priority and commitment by government to continue to actively regulate the area and manage the cumulative tension between individual and collective rights to personal healthcare information, human identity and experience is

[140] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10.

[141] See Kenneth Newton and Pippa Norris, 'Confidence in Public Institutions: Faith, Culture, or Performance?' in Susan Pharr and Robert Putnam (eds), *Disaffected Democracies* (Princeton University Press, 2000): at 31; Russell Hardin, 'The Public Trust' in Susan Pharr and Robert Putnam (eds), *Disaffected Democracies* (Princeton University Press, 2000): at 52; Clive Hamilton and Sarah Maddison (eds), *Silencing Dissent* (Allen & Unwin, 2007).

compromised by increasing global capitalist forces that insist upon objectifying individuals by transforming them into tradable commodities.[142] It is therefore imperative that agreed governance regulations that *preference* consumer voice and choice, in the governance process and privacy regulations, be established and supported, before the federal government ultimately relinquishes the ongoing management (and privacy rights) of the *PCEHR* and e-health system's 'command and control' into the hands of private industry interests.[143]

VI. TECHNICAL MEASURES

In conjunction with the development of privacy law and governance protection plans, the Australian Government predicts that advancing sophisticated technology measures—'functionality and network interoperability'—and design capabilities will further enhance *PCEHR* and e-health privacy, and security supporting governance within the proposed system.[144] It is anticipated that a multi-layered approach will safeguard the *PCEHR* system and will incorporate both technical and non-technical controls, which include accurate authentication, rigorous security and requirements that healthcare providers and organisations comply with specific *PCEHR* system business rules and relevant legislation.[145]

---

[142] See Huw Beverely-Smith, *The Commercial Appropriation of the Personality* (Cambridge University Press, 2002); see also the *International Labour Organisation* (ILO), ILO Constitution, which declares that 'labour is not a commodity'; see Colin Fenwick and Tonia Novitz (eds), *Human Rights at Work* (Onati International Series in Law and Society, 2010) vii.

[143] See Dryzek and Dunleavy, *Theories of the Democratic State*, above n10. Dryzek outlines and discusses the position and importance of 'command and control' mechanisms relating to governance: at 20.

[144] See NEHTA, *Concepts of Operations*, above n77: at 3; see generally on the importance of security law in Australia and its growth in modern society - Rick Sarre and Tim Prenzler, *The Law of Private Security in Australia* (Thomas Reuters, 2nd ed, 2009).

[145] NEHTA, *Concepts of Operations*, above n77: at 12.

The *Review* concurs with technical security measures outlined in the 2011 *Concepts of Operation,* including the establishment of a Commission on Information and Security Risk Assessment to oversee the end-to-end flow of consumer information. It also recommends that 'findings and mitigation actions be reviewed and agreed by the Privacy and Security Committee.'[146] However, the most contentious recommendation is for the immediate update of the *MyHR* strategy, to enable 'decentralisation' of information across multiple data repositories, using the *HI* number.[147] These proposed function and interoperability measures display a disregard for long-term privacy, security planning and public risk considerations outlined in the *Concepts of Operation* document,[148] by promoting the set-up of the *PCEHR* system and a 'wait and see' approach for identifying security and privacy problems as they arise. This appeal to *immediacy*, based on the *PCEHR* regime commercial demands, effectively puts 'the cart before the horse' in relation to designing 'gold standard', embedded technical measures protecting individual healthcare information security and privacy rights.[149]

Another important consideration informing the *PCEHR* system technical measure debate, is that technology 'evolution' will 'self-regulate', and that computer and information technology is becoming more sophisticated, enabling it to predict and solve its own function (such as security and privacy) limitations.[150] There are

[146] See *Royle Review*, above n1 Rec. 16.

[147] Ibid Rec. 31.

[148] Ibid Rec. 32.

[149] See Ann Cavoukian, *Privacy by Design in an Age of Big Data*, above n84; Ann Cavoukian, *Embedding Privacy into Healthcare Information Technology*, above n83.

[150] See chapter 3, pp68-97 for discussion technology; NEHTA, *Concepts of Operations*, above n77: at 77; Bryan Foster and Yvette Lejins, 'E-Health Security in Australia: The Solution Lies with Frameworks

numerous counterarguments to the proposition that individuals can rely on technology to 'self-regulate' privacy and security values beyond their own fiscal interests.[151] For instance, there is ample evidence to suggest that business entities have very good reasons, such as corporate reputation and economic interest, to build consumer trust by embedding privacy.[152]

On the other hand, there exist numerous examples of how privacy is lost because it is too late, too difficult and too costly to upgrade earlier programs that have not embedded adequate privacy.[153] Indeed, it is also highly predictable that it may not be in the interest of governments and industry to discard information it has previously collected or dismantle existing systems.[154]

Limitations to the 'self-regulate' argument include that technology is not a passive or 'neutral utility' player.[155] Technology designs and programs reflect dominant political and economic ideology that may or may not support individual privacy protection rights or democratic ideals. What becomes embedded in technology programming will often reflect many different social activities, which

---

and Standards' (Paper Presented to Australian eHealth Informatics and Security Conference, 2013); See generally Don Ihde, *Philosophy of Technology* (Paragon Publication, 1993); Paul Barren, "The Future of Computer Utility" (1967) *The Public Interest Policy* cited in Evgeny Morovoz, "The Real Privacy Problem", above n4: at 2.

[151] See Evgeny Morozov, "The Real Privacy Problem", above n4: at 3; Daniel Solove, *The Digital Person* (New York University Press, 2004); Daniel Solove, Marc Rotenberg and Paul Schwartz, *Privacy, Information, and Technology* (Aspen Publishers, 2006); Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008); Tal Zarsky, "Mine Your Own Business", above n84.

[152] See Ann Cavoukian, *Embedding Privacy into Healthcare Information Technology*, above n83; Ann Cavoukian, *Privacy by Design in an Age of Big Data*, above n84.

[153] See Eugeny Morozov, "The Real Privacy Problem", above n4.

[154] Ibid 3; Daniel Solove, *The Digital Person*, above n151: at 131; see generally, Viktor Mayer-Schonberger, *Delete* (Princeton University Press, 2009).

[155] See chapter 3, pp83-88 for discussion on technology and technology 'neutrality'; see also ALRC, Discussion Paper 72, above n56: at 342.

include the creation of commercial consumer activity, surveillance dossiers and satisfying government and private enterprise information gathering needs.[156] The problem is that in an increasingly global, economic society, where information is power, democratic ideals such as civil liberties and privacy rights are under constant threat and in some circumstances, democratic processes are compromised or indeed sacrificed.[157]

VIII. CONCLUSION

As a consequence of recent economic shifts, citizens must give careful consideration to competing healthcare stakeholder interests and decide how to protect their long-term interests and positively influence the new electronic healthcare regime.[158] The 'balance' between individual and collective rights is under threat on a number of levels, including the election of the present federal government, because of its health restraint and rationalisation policy. This will weaken the introduction of robust governance mechanisms that have already been put in place by the previous government to prioritise individual privacy protection rights within the new electronic healthcare regime. It also adds to the ongoing inconsistency and fragmentation of the proposed e-health and privacy protection scheme, and will ultimately affect national harmonisation considerations.

---

[156] See Daniel Solove, *Nothing to Hide* (Yale University Press, 2011) 21.

[157] See Eugeny Morovoz, "The Real Privacy Problem", above n4.

[158] See Richard Au and Peter Croll, 'Consumer-Centric and Privacy-Preserving Identity Management for Distributed e-Health Systems' (Paper Presented at 41st Hawaii International Conference on System Sciences, 2008); see Gaze and Jones, *Law, Liberty and Australian Democracy*, above n34.

Australia operates under democratic principles that guard against repressive and nondemocratic activity and practices. The right to vote and the right to question any mechanisms (even inevitable modern technology progress) that may be complicit in denying (intentionally or otherwise) citizens' rights to expect transparent and accountable processes, by governments or anyone else operating in Australia, is fundamental to democratic principles. Denying citizens a proper voice in the *PCEHR* and e-health process, transferring central power for the continuing leadership and management of the system to private industry, and supporting further clinical control over individual personal electronic healthcare records, is questionable and democratically dangerous.

The *Royle Review*, whilst putting forward some very positive ideas for progressing *PCEHR* systems demonstrates just how far the present government has moved away from the foundational concept of inclusive consumer involvement in his or her *PCEHR* record creation. This is a retrograde step and further contributes to the ever-diminishing, democratic rights of citizens, particularly in an increasing global environment. The rise of global market liberalism and neo-pluralistic polity threatens the very core of civil society, as powerful economic actors insist upon the 'commodification' of citizens and argue in favour of the necessity for unfettered political/social power.[159]

In response to broader political and economic expansionism in Australia, it is not suggested that home state regulation provides the panacea for *trans*-national

[159] See Jaron Lanier, *You are Not a Gadget* (Alfred Knopf, 2010).

problems, but rather that governance is complex and needs to be tackled on a variety of jurisdictional and normative planes. It is recognised by governance scholars, Simons and Macklin, that the long-term limitations of home state regulations do not necessarily address the governance gap.[160] Nevertheless, the lack of requisite consensus for establishing international responses is not solved by shifting 'command and control' away from domestic mechanisms and relocating it in commercial business and *MNE*'s.[161]

Unilateral home state governance and regulation (such as individual privacy rights protection) is a crucial part of a multi-level, multi-jurisdictional project and will, if democratically supported, contribute to the eventual development of consensus at the domestic and international level for a global response to the problem of corporate impunity.[162]

To conclude, it is recognised in this chapter that despite prior legislative responses and advances in the new electronic healthcare regime, essential and considered developed governance measures have not yet been achieved, nor implemented, given that the *PCEHR* system has been operational since 2012. The lack of governance progress in this area, at this late stage, is inexcusable. Governance mechanisms and assurances represent an essential key privacy element for all stakeholders. Hence, the proposed trilogy of legislation, technology measures and governance, despite much progress over the last decade towards implementation of

[160] Simons and Macklin, *The Governance Gap*, above n10: at 179.
[161] Ibid 20-21.
[162] Ibid 21.

the *PCEHR* system and the work of the *Review*, is still inadequate, because it fails to provide the necessary individual privacy protection 'balance' promised to citizens by past Australian Governments.

Consequently, the thesis argues that it is time to rethink and restructure the *PCEHR* and e-health governance strategy in light of advancing, global, political, economic and social tensions and to identify what governance mix best reflects and balances the needs of all stakeholders.[163] In this ever changing context, it is argued that the introduction of a *Council* will restore representative balance and positively progress the e-health governance system. The following, concluding chapter, sets out the new, proposed governance structure, arguing its relevance and significance to further advance privacy protection, as well as ensuring adequate accountable and transparent democratic processes, to restore the necessary balance of citizen rights.

[163] See Bridie Jabour, 'Australian Authors Join Call for UN Bill of Digital Rights to Protect Privacy' *The Guardian* (UK), 10 December 2013, 1.

CHAPTER 7

THESIS SUMMARY AND CONCLUSION

The thesis has identified and analysed the political, economic and social development and implementation of *PCEHR* and e-health Systems as well as health privacy protection measures in Australia over the last few decades; arguing its continuing relevance and impact on our day-to-day lives. Earlier chapters provide a detailed analysis of the evolution and theoretical advancement of health, technology, law, governance and privacy in order to contextualise and 'frame' the thesis proposition promoting the introduction of a *Council* and arguing why this significant change is necessary in light of recent Australian Government healthcare policy changes and moves towards embracing rapidly advancing communication technology and globalisation.

The thesis chapters also reflect not just the developing and shifting physical manifestation of the new Australian health and healthcare digital regime but highlight the multifarious problems and new conceptual reality of health and technology that now drives widespread 'network' linked communication system adoption in modern day knowledge and information economy era.[1] This chapter concludes the thesis argument by summarising the earlier chapter information in order to further advance

[1] See Jeffery Rosen, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror" (2004) 46 *Arizona Law Review* 607; David Watkins, 'Sony Apologises for PlayStation Privacy Breach and Boosts Security' *Herald Sun* (UK), 2 May 2012, 1.

the thesis proposition that individual healthcare privacy is threatened by the 'shared' electronic health regimes and that more must be done by the Australian Government to foster citizen trust and confidence in e-health and ensure adequate privacy rights protection in modern information era.[2]

The early chapters of the thesis open with background information and an outline of the Australian Government's rationalisation policy for introducing the new electronic health regime, including an outline of the contextual time frame (2000-2014) of the e-health evolution. The thesis subsequently moves through time to the present federal Government's political and economic policy changes and challenges, which includes less government oversight of the e-health systems in a move towards promoting greater healthcare privatisation, commercialisation and devolution practices.[3] The thesis reconnoitres the continuing 'blurring' of lines between political and economic power roles (and actors), which captures the continuing Australian and worldwide erosion of traditional government governance mechanisms such as public sector organisations and independent bodies thus further impacting on democratic considerations such as civil liberties and human rights privacy protection.[4]

---

[2] Michael Carey and Merrilyn Walton, 'On Trust' in Ian Kerridge, Christopher Jordens and Emma-Jane Sayers (eds), *Restoring Humane Values to Medicine* (Desert Pea Press, 2003): at 166; Adam McBeth, "Privatising Human Rights: What Happens to the State's Human Rights Duties When Services are Privatised?" (2004) 5(1) *Melbourne Journal of International Law* 133.

[3] See Waleed Aly, 'Coalition Needs a Heart Transplant, Not a Facelift', *Sydney Morning Herald* (online), 6 February 2015, 30.

[4] See Paul Smith, 'Dutton's Legacy: The Anti-Health Minister' *Australian Doctor* (Australia), 12 January 2015, 18; see also Bridie Jabour, 'Australian Authors Join Call for UN Bill of Digital Rights to Protect Privacy', *The Guardian* (UK), 10 December 2013, 1; See also Andreas Georg Scherer and Guido Palazzo, "The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy" (June 2011) *Journal of Management Studies* 48:4; Australian Government, *Serious Invasions of Privacy in the Digital Era:* Discussion Paper 80 (March 2014).

The analysis within the chapters also informs the ongoing debate about the growing 'symbiotic' relationship between health and technology by exploring 'networking' systems that manipulate how people communicate with each other in an increasingly borderless virtual reality.[5] This shift towards digital 'collection and sharing' of personal healthcare information is in direct contrast to how healthcare delivery has been organised in Australia, especially in relation to traditional legal and ethical reliance by patients on doctors to maintain confidentiality and protect privacy of personal healthcare records.[6]

In combination with thesis exposition of modern day 'shared health and technology' system development is the concurrent rise of major privacy and security problems such as increasing intrusive surveillance mechanisms and expanding reliance upon national security measures.[7] Chapter 5 explores federation and constitutional issues, common law and statutory responses and development of health, e-health and privacy area across the nation. It highlights the importance of national cooperation and identifies the advantages relating to legal 'harmonisation' in light of the changes that Australia is now facing. It achieves this by tracing the federal,

---

[5] See chapter 3, pp70-97 for discussion of technology and 'networks'; See generally Asher Moses, 'Software Takes Brain Power out of Hacking' *The Sydney Morning Herald* (Australia), 28 July 2011, 23.

[6] Paul Smith, 'Give Me Socialised Medicine Any Day', *Australian Doctor* (online), 17 August 2009 (online) http://www.australiandoctor.com.au/opinions/paul-smith (viewed on 3/2/2015); Angela Palombo, 'Record Creation and Access: The Impact of Legislative Changes' in Ian Freckelton and Kerry Petersen (eds), *Disputes & Dilemmas in Health Law* (The Federation Press, 2006): at 639; Jay Katz, *The Silent World of Doctor and Patient* (The John Hopkins University Press, 2002); Megan Richardson, "Whither Breach of Confidence: A Right of Privacy for Australia?" (2002) 26 *Melbourne University Law Review* 20.

[7] See chapter 3, pp79-90 for discussion of surveillance; chapter 6, pp231-234 for discussion of security technology measures and *Privacy by Design*: at pp203-209; see Australian Government, *Serious Invasions of Privacy in the Digital Era,* above n4; ALRC, *Surveillance: Final Report*: Report 108 (May 2005). See also David Watkins, 'Sony Apologies for PlayStation Privacy Breach and Boosts Security', above n1: at 2; The Royal Australian College of General Practitioners (RACGP), *Computer and Information Security Standards* (October 2011).

State and Territory legal responses to these powerful political, economic and social changes. Significantly this legal analysis makes the important observation that 'harmonised' law creation activities is vital to Australia's future, and that any appeals to common law must contribute to creation of proactive protective mechanisms if we are to adequately protect privacy rights in Australia.

Chapter 6 develops this theme further by outlining the current legal and governance responses to *PCEHR* and e-health systems implementation. This pre-emptive approach to governance mechanisms is particularly important given all the political and social changes that are occurring in Australia, especially in relation to the growth of neo-capitalism and the adoption of modern global digital economy, which threaten individual human rights and democratic processes. [8]

Interrelated and interwoven throughout the chapter analysis is the building of the argument towards the proposition that a *Council* be introduced in order to progress individual privacy protection and promote democratic processes in the e-health area. Given the progressive context of e-health systems, it is argued that it is time to put the pieces of the 'puzzle' together so that the 'story' of electronic health regime and adequate individual privacy protection has a satisfactory ending for all national stakeholders, particularly consumers.

[8] See Evgeny Morozov, "The Real Privacy Problem" (22 October 2013) 116(6) *MIT Technology Review* 32. Morozov argues that 'both capitalism and bureaucratic administration are convinced that the spread of digital networks and the rapid decline in communication costs represent a genuine new stage of human development': at 33. 'For them, the surveillance triggered in the 2000s by 9/11 and the colonisation of these pristine digital spaces by Google, Facebook, and big data were aberrations that could be restricted or at least reversed': at 33.

As argued throughout the thesis, the need for these changes to health law/regulation have in large part been driven by advancing technology, which favours knowledge and information systems for rapid and cheap sources of information and communication.[9] Generally, advanced communication system usage is highly desirable as a means of gaining an economic and competitive advantage in the new information driven world. However, there are a number of unforeseen side-effects to its acceptance, for instance the very concept of what it means to be human are challenged as are perceptions of established traditional local and community values and communication systems.[10]

In order to advance this point about the significance of controlling technology rather than allowing it to control recipients, the theoretical bases for technology is explored in chapter 3. The chapter highlights three major reports published over the last decade, which consistently indicate that in order to progress *PCEHR* system healthcare consumers must continue to be visible, heard and occupy a driving force

---

[9] See Matthew Knott and David Wroe, 'Laws to Reduce Hacking Risk Under Metadata Plan' *The Sydney Morning Herald* (Australia), 1-2 November 2014, 9. This newspaper report discusses the Abbott Governments plan to introduce new laws to stop internet companies storing customer's records for two years on cheap overseas servers that are vulnerable to hacking by criminals and foreign governments: at 9; see Review Panel, Richard Royle, Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* ('*Royle Review*') (December 2013). On 3 November 2013, the then Federal Minister for Health, Peter Dutton, announced a review of the *PCEHR* system by a small panel of health and IT experts (no consumer representation). As outlined in Chapter 6, the panel made 38 recommendations, which it presented to the Minister in December 2013. One recommendation (Rec.31) by the *Review* is for: '[Immediate] update [of] the *MyHR* [*PCEHR*] strategy to actively enable decentralisation of information across multiple data repositories, with information being linked using the Healthcare Identifier (HI) number': at 17. It also recommended that *PCEHR* and e-health data storage repositories regulations should be extended to include overseas companies (storage repositories) in a bid to be more competitive in the marketplace. This is clearly contrary to the numerous promises and legislation (*Healthcare Identifiers Act*, *PCEHR Act*) by previous Australian Governments not to let personal health information be subject to storage in repositories where privacy laws may be far less robust, harder to enforce, leaving sensitive personal health records vulnerable to other inappropriate uses that were not anticipated by those consumers who were prepared to freely provide healthcare information.

[10] See chapter 3, pp70-97.

in the adoption process.[11] In the CSC Healthcare Research Report – *A Rising Tide of Expectations* –consumer involvement is highlighted and it is noted that 'the consumer voice in particular, has not yet been strongly heard in relation to e-Health.'[12] Similarly the *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System (Concepts of Operations),* also contends that 'central to the *PCEHR* System is the concept of [consumer] personal control and participation' and that it is essential to gain consumer 'trust and confidence' in the system in order to make it worthwhile.[13] Additionally it is articulated in *A National Health and Hospitals Network for Australia's Future*, which amongst its recommendations also supports a need for a 'unified approach' by all Australian Governments to health and the new health regime.[14] It also recognises that consumer support and involvement in the system is essential if it is to be used successfully.[15] The important theme of consumer 'trust and

---

[11] Australian Government, National Health Reform Committee (NHRC), *A National Health and Hospitals Network for Australia's Future* (2010); NEHTA, *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* (September 2011); Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*: Issues Paper 43 (October 2013); Australian Law Reform Commission (ALRC), *Review of Australian Privacy Law:* Discussion Paper 72 (2007); ALRC, *For Your Information: Privacy Law in Australia* (2008); ALRC, *Review of Privacy*: Issues Paper 31 (2006).

[12] CSC Healthcare Research Report, *A Rising Tide of Expectations Australian Consumer's View on Electronic Health Records – A Necessary Ingredient in Healthcare Reform* (July 2010). CSC is a global leader in providing technology enabled business solutions and services in many industries. Its research seeks to start the process of informing and eliciting Australian e-health debate (note: CSC is the full title of the company): at 1.

[13] NEHTA, *Concepts of Operations,* above n11: at 15.

[14] NHRC, *A National Health and Hospitals Network for Australia's Future: Delivering the Reforms*, above n11. Under these reforms, the National Health and Hospitals Network (NHHN) will create a single national unified health system which is nationally funded: at 4. 'A core element of the National Health and Hospitals Network will be strong national standards and transparent reporting that is nationally consistent and locally relevant': at 8; see also COAG, *National Healthcare Agreement 2011.* This agreement defines the objectives, outcomes, outputs and performance measures, and clarifies the roles and responsibilities that will guide the Commonwealth and States and Territories in delivery of services across the health sector; John Paterson, "Australian Health Care Agreements 2003-2008: A New Dawn?" (2002) 6 *Medical Journal of Australia* 177 [COAG 2003-2008 agreements emphasised a focus on provision of best care and health outcomes rather than jurisdictional boundaries, with jurisdictions working cooperatively to advance community health and well-being].

[15] See National Health and Hospitals Network (NHHN), *A National Health and Hospitals Network for Australia's Future*, above n11: at 50.

confidence' arises again and again in various other reports generated over the last ten or so years such as the Australian Law Reform Commission's (ALRC) —*Review of Australian Privacy Law*.[16]

A later 2013 *Review of Personally Controlled Electronic Health Records* report,[17] challenged that important notion of *consumer-centric* involvement, by recommending that a radical shift occur that would minimise public sector direct engagement and expand multi industry and professional control mechanisms in the future *PCEHR* governance of the system. This shift recommended by the *Royle Review* would consign consumer involvement to that of *steward* of their personal health information and elevate other stakeholders – 'the panel wishes to retain the engagement of the consumer as *stewards* of their own health … while recognising the needs of the clinicians.'[18] It is argued in this thesis that this power shift would result in disempowerment of consumers whilst further promoting and guaranteeing greater professional and industry interests (and power) in directing and controlling the e-health governance process (including privacy).[19] Thus the promised objective of 'balancing the needs of individual and collective privacy interests' in this area would be further compromised by favouring and empowering professional and private industry actors.[20]

---

[16] ALRC, Discussion Paper 72, above n11: at 105.

[17] See *Royle Review*, above n9: at 19.

[18] Ibid.

[19] Paul Smith, 'Who Are the Real Winners in the e-Health Pay Deal?' *Australian Doctor* (Australia), 24 August 2012, 18; Paul Smith, 'Where is Debate on the Health of Our Nation?' *Australian Doctor* (Australia), 13 August 2013, 18; Paul Smith, 'Is the Private Health Push in the Public Interest?' *Australian Doctor* (Australia), 2 April 2014, 18.

[20] Australian Government, *Concepts of Operations*, above n11: at 61; Australian Government, National Health Reform Council, *Health Online: A Health Information Action Plan for Australia* (2001): at 2.

Demonstrated throughout the thesis, is the argument put by economists and IT experts that rapid political, economic and social change is inevitable.[21] While it is acknowledged that change is indeed unstoppable, a 'balanced' and well thought through approach towards progress can be envisaged: one which better manages change in a way which truly reflect the interests and rights of all parties subject to that change. In order to achieve this goal there are a number of non-negotiable *PCEHR* and e-health commitment criteria that citizens and Government must agree upon in order to initiate positive and inclusive change outcomes that preference community interests and social values. These non-negotiable *PCEHR* and e-health governance commitments include – that privacy is the first priority of government, and that present and future decisions about *PCEHR* privacy governance remain organised through elected Governments (not transferred to private organisations) and continue to operate as transparent and accountable processes.[22]

Furthermore it is posited that if the private sector is poised to take further advantage of the new electronic health regime that their involvement at all levels be subject to open transparent and accountable processes and that preference be given to amplifying citizen 'voice' and influence because the public represents the largest group affected by these proposed changes. It is also imperative, particularly in the information economy that the public not be reduced to a mere recipients or receivers

[21] See chapter 2: at pp38-67 and chapter 3: at pp70-97 for discussion on government health policy and technology.

[22] See Scherer and Palazzo, "The New Political Role of Business in a Globalized World", above n4; Beth Gaze and Melinda Jones, *Law, Liberty and Australian Democracy* (The Law Book Company, 1990); see generally Senate Standing Committee on Constitutional and Legal Affairs, *A Bill of Rights for Australia?* (1985).

of healthcare products or services, but have the option to be involved in decision-making at the 'grass roots' level.[23] Consequently a wider commitment to representation of viewpoints must be considered in order to elicit a 'selection of trusted personnel who will represent the views of the target audience and who have the authority and accountability to act',[24] not only for economic stakeholders but also citizens.

As highlighted in chapter 6, the *Royle Review* provides an interesting and in some circumstances relevant framework for how *PCEHR* and e-health governance could be organised and modelled in the future. Some of the *Review* recommendations are worth considering in the current economic environment. However, it is also recognised that hidden within this *Review* is the recommendation that health industry and health professionals be elevated to powerful decision-makers, that Government overview Departments and bodies be rationalised and given a secondary role, and that citizens participation be reduced in that they should 'trust' professional and industry experts appointed to committees to make informed decisions and manage the process with reduced oversight.[25]

Problematic to the *Review* is the fact that it does not demonstrate nor appeal to any theoretical conceptual argument or substantial evidence on which to base its arguments or recommendations for this very radical engagement 'shift' from

[23] Michael Carey and Merrilyn Walton, 'On Trust' in Kerridge, Jones and Sayers, *Restoring Humane Values to Medicine*, above n2: at 166.

[24] *Royle Review*, above n9: at 20.

[25] Ibid 14.

traditional *consumer-centric* to *industry/professional-centric* stakeholders preference;[26] although it does indicate that the main consideration is about progressing the system and is economic in nature. Other *Review* arguments used to justify this radical industry/professional focus 'shift' emphasise the poor consumer and healthcare provider up-take of the system. It suggests that the reason for healthcare provider and consumer low level up-take of e-health relates to the lack of stakeholder feedback, governance and *NEHTA* management style.[27] All of which can be disputed as suppositions not entirely correct or sustainable by evidence-based criteria.[28]

However what the thesis acknowledges is that the *PCEHR* system has ostensibly failed to attract the type of commitment that Government and industry anticipated because the public is far from *convinced* that giving up their 'rights' (real or perceived) to 'control' their personal health information simply provides no or very limited benefit for them, despite being reassured over the last twenty years that the *PCEHR* system is beneficial and will continue to protect their interests. If indeed this is part of the problem, then mandating compliance such as introducing 'opt-out' rather than 'opt-in' consumer participation recommended by the *Review* will undoubtedly progress the system but it will ultimately fail to achieve its expected

---

[26] *Royle Review*, above n9. The *Review* states that strong international evidence exits that data aggregation and management has led to better outcomes and appeals to an American integrated care consortium example based in Oakland California. However the *Review* provides absolutely no evidence-based research reference to actually demonstrate or indeed support this 'fact' statement: at 13.

[27] Paul Smith, 'Exodus of Doctor's Adds to E-Health Uncertainty' *Australian Doctor* (Australia), 28 August 2013, 18; Deb Richards, 'Medical Groups Snubbed by E-Health Initiative' *Medical Observer* (Australia) 25 November 2005, 9 [Where Dr Haikerwal stated that: 'We can't wait for these guys [NEHTA] each time to screw up and ask us to help bail them out': at 9]; Paul Smith, 'Dutton's Legacy: The Anti-Health Minister' *Australian Doctor* (Australia), 12 January 2015, 18.

[28] ALRC, Discussion Paper 72, above n11.

purpose of public confidence/acceptance if there is no consumer commitment or 'ownership' of the system. For instance, some individuals will simply give what they consider to be necessary (or wrong) information to their healthcare providers.[29]

It is also suggested that the primary reason why doctors have now come on board in relation to *PCEHR* system implementation is because they have been assured by Government of continued dominance over the implementation and control of the *PCEHR* and e-health system.[30] This observation can be evidenced by the new proposed role of the Independent Advisory Council (IAC) (consisting primarily of healthcare professionals), which according to *Review* should be retained. The review recommends that 'The Independent Advisory Council (IAC), with existing membership, continues to operate under its terms of reference as identified in the IAC Charter' (31 August 2012). This recommendation changes the IAC current line of reporting to one that would allow a direct line to the Federal Minister and no longer require the IAC to report to the System Operator, *NEHTA* or any other new bodies such as the Australian Commission on Electronic Health.[31] Thus for this particular Advisory Council (IAC) there would be virtually no external (other than the Health Minister) monitoring of its activities. Indeed this situation does not embrace

[29] See, eg, Omer Tene and Jules Polonetsky, "Big Date for All: Privacy and User Control in the Age of Analytics" (April 2013) 11(5) *Northwestern Journal of Technology and Intellectual Property* 239: at 245, 260-263.

[30] See *Royle Review*, above n9. The *Review* recommendation is for exclusive advisory role of IAC: at 26, 79.

[31] Ibid. There are a number of related issues that emerge concerning the *Review* recommendation about the new IAC, its independent, lack of external overview and oversight (transparency and accountability), and existing membership appointments including its proposed function and direct line access to Health Minister.

transparency and accountability in any way and would ultimately result in exclusivity and loss of public overview of the process.

Chapter 6 analyses of *PCEHR* and e-health governance also suggests that the answer to dealing with these dilemmas is not found by expecting corporations to manage or direct their attention to developing extended social and political values via extended Corporate Social Responsibility (*CSR*).[32] This extreme suggestion quite clearly runs counter to democratic participation, and would result in hidden elite management and further diminish or indeed negate democratic principles and ideals of governance transparency and accountability processes. Nevertheless, it cannot be ignored that the new modern economic constellation era has continued to *blur* the lines between traditional political and economic power roles and that there are now not just government but multi-layered industry and professional pluralistic actor pressures vying to control how the new world order will be governed, or indeed whether or not it should be governed or managed at all.

Decentralising government, rationalising resources and services such as the Information Commissioner or engaging in exclusive relationships with corporations and/or other organisations (stakeholder actors) to ultimately take over responsibility for running society and determining citizen participation or rights is not an option that Australia should be entertaining. We must reaffirm our commitment to democratic ideals and processes that promote shared community values and advance the notion of *inclusive* citizen discourse in the new information technology system.

[32] See Scherer and Palazzo, "The New Political Role of Business in a Global World", above n4.

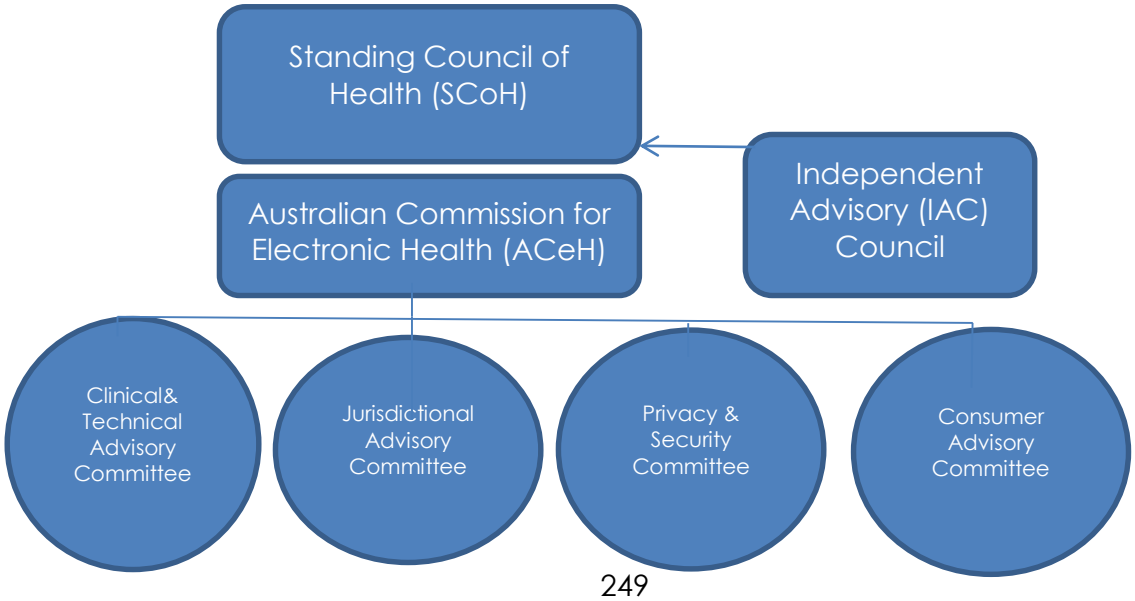
The thesis posits that a *Council* can be viewed as a beginning stage of this collective idea by adopting this progressive measure. A *Council* represents a new way of perceiving how *PCEHR* and e-health governance must be conceptualised and progressed now and in the future.

The adoption by the Australian Government of a *Council* to further strengthen consumer privacy protection is highly recommended. Additionally, it provides an extra layer of public administrative sector transparency and encourage democratic citizen participation in relation to ongoing protection of privacy rights in an era that increasingly needs to make us more visible and vulnerable to the 'unwanted gaze' of an increasing number of third party actors.

I. DECONSTRUCTING THE 'ROYLE REVIEW' RECOMMENDATIONS

In order to advance the idea of a *Council* it is necessary to diagrammatically reiterate what the *Royal Review* proposes in relation to *PCEHR* governance structure and compare its recommendations with the revised thesis proposition.

The Review sets out its structural recommendation as follows: Diagram 1.



A basic *Review* assumption is that the government, public service and consumer involvement in e-health systems should be minimised: '[t]he government's role in e-Health system should be limited, focused on developing essential standards … with the requirements of vendors and end-users being the primary consideration in this process.'[33] And that a:

> Revised body needs to have relative independence from State and Federal Government departments to ensure it is balanced and represents the needs of multiple key stakeholders to facilitate the elements of e-health delivery by a healthy private sector.[34]

Further the *Review* contends that 'ideally there should be an independent System Operator and an Independent Advisory Committee and that *clinical oversight and control* [emphasis added] is required.'[35] The *Review* argues that since the handover to the Department of Health and Ageing – 'now the Department of Health (DoH) – governance has been reduced to essentially non-existent'. Given these observations about the Department of Health, the above statement represents an extraordinary representation and interpretation of present events.[36]

The Australian Commission for Electronic Health (*ACeH*) would replace NEHTA and be established as a Statutory Authority reporting directly to the Standing Council on Health (*SCoH*). Its role would include development and execution of e-health strategies within the policy framework set by the Federal Minister of Health. The *ACeH* would centralise the system operation of the *MyHR* (new proposed name

---

[33] *Royle Review*, above n9: at 79.

[34] Ibid 26.

[35] Ibid 79.

[36] Ibid.

for *PCEHR* System) to the Department of Human Services, under contract from *ACeH*. It would set and implement funding priorities for e-health initiatives, provide and manage vendor accreditation process and provide frameworks and requirements to allow value adding vendors to integrate with *MyHR*. It would monitor performance, adoption and management of e-health systems, including oversight of the System Operator. The proposed composition of the *ACeH* would include: Chair (nominated by the Federal Minister for Health), industry representative, private hospital operator, Jurisdictional representative (nominated by the Australian Health Ministers Advisory Committee (AHMAC)); general practitioner; medical specialist; pharmacist; allied health professional; health software industry representative; registered Nurse; aged care operator and consumer (nominated by the Consumer Advisory Committee).

According to the blueprint in the *Review*, the *ACeH* would establish a number of advisory sub-committees in order to ensure consideration of issues under discussion.[37] One proposed advisory committee is the Clinical and Technical Advisory Committee, which would bring together IT technical experts and clinicians to enhance e-health efficiency and effectiveness of clinical care as well as advise the *ACeH* on clinical and related technical functionality of the *MyHR* with the intention of increasing utility and functionality as well as investments in the *MyHR*.[38] Proposed membership of the Clinical and Technical Advisory Committee would include: *ACeH* Board member (General practitioner); specialist medical practitioner, pathology representative, diagnostic imaging representative; pharmacist; software industry

[37] *Royle Review*, above n9: at 22-23.
[38] Ibid 23.

representative; rural doctor; private and public chief information officer representative, member of the Consumer Advisory Committee and Department of Human Services representative (as system operator).[39]

Recommendations are also made to establish a Jurisdictional Advisory Committees to *ACeH*, with a proposed membership of Chair (to be the Chair of *ACeH*); Jurisdictional Health representatives (nominated by the Director General of each Jurisdictional Health Department) and a Federal Department of Health representative. The role of the Jurisdictional Advisory Committee is to provide advice on all issues directly relating to e-health.[40] The *Review* also envisages establishment of a Privacy and Security Committee to *ACeH*, which would be responsible for examining legal and related issues regarding the *MyHR* including ownership, copyright, security, liability, confidentiality and data privacy. The membership of this Committee would include: Chair to be federal Department of Health representative on the *ACeH* Board; general practitioner; medical specialist; medical insurer representative; software security expert; medico-legal representative; representative of the Privacy Commissioner and consumer representative.

The proposed Consumer Advisory Committee to *ACeH* will, according to the *Review* enhance efficiency and effectiveness of clinical care; advise the Board on issues to break downs in collaboration or barriers to better execution; and facilitate consumer participation in healthcare. Membership of this Committee would consist of 13 members and include: a Chair; with only 'up to three consumers representing

[39] *Royle Review*, above n9: at 24.
[40] Ibid.

different consumer groups'; general practitioner; specialist medical practitioner; nurse practitioner; allied health professional; Department of Human Services representative (as System Operator) and Clinical and Technical Advisory Committee member representative.[41]

The thesis accepts that a Consumer Advisory Committee be established but firmly rejects the *Review* recommendation relating to its intended role, its suggested sub-committee status level in the proposed structural hierarchy, its membership, and its limited line of reporting role (*ACeH*). The proposed Consumer Committee membership is rejected for lack of proper consumer representation. This is on the basis that it unduly preferences professional representation within what should be a *consumer* forum. The *Review* proposal of consumer representative membership (up to 3 members) is clearly inadequate in order to capture the diverse range of consumer groups concerns regarding e-health service delivery and privacy issues such as Aboriginal, mental health, disability, aged care and remote area services.

Arguably, one of the most contentious *Review* recommendations, alongside the reduction of consumer representation and involvement in the *PCEHR* and e-health system, is maintenance of the Independent Advisory Council (*IAC*) with altered reporting line, direct to the Federal Minister for Health. As earlier mentioned, the *Review* argues that the current reporting line of the *IAC* be changed to the federal

[41] *Royle Review*, above n9: at 23-24.

Minister of Health and that current *IAC* continue because it 'has proved to be a useful forum for oversight of the PCEHR process.' [42]

II. THE NEED FOR A COUNCIL TO ENSURE TRANSPARENCY

Unlike the *Review* model outlined above, which preferences health industry and healthcare professional groups by reducing consumers to the status of sub-committee advisory group, a *Council* as proposed in this thesis would reprioritise and restructure the *Review* recommendations by emphasising citizen visibility, 'voice' and participation. It would strengthen consumer involvement, encourage democratic citizenship, and subsequently healthcare privacy protection. It would be a cost effective mechanism that adds an extra layer of public administration sector transparency and provide a much needed 'forum' and 'balance' in the present and future governance and management of the *PCEHR* and e-health systems.

Thus the overall restructure proposed in this thesis of the *Review* blueprint would shift the focus back to consumers, by spotlighting the largest group most affected by the electronic healthcare changes. The importance and ongoing participation of health industry and professional groups to work in partnership with consumer expectations is also supported in the proposed governance arrangement mechanism.

---

[42] *Royle Review*, above n9: at 26; see Paul Smith, 'Exodus of Doctor's Adds to E-Health Uncertainty' *Australian Doctor* (Australia), 28 August 2013, 18; Paul Smith, 'GP E-Health Funding Win' *Australian Doctor* (Australia), 31 August 2012, 1. This rationalisation used by the *Review* for maintaining existing membership of the Independent Advisory Council, clearly does not mention nor take into account the mass walk-out and resignation of the medical practitioners from this Council in protest in 2013.

The creation of a *Council* would operate on a different dimension than other existing independent bodies such as the OAIC. As noted in chapter 5, the *PCEHR* and Privacy legislation expands the role of the Information Commissioner in its capacity to handle complaints and set guidelines for the public and private sector in relation to information privacy.[43] This independent administrative overview role of information privacy rights and protection is taken seriously by the Commission, which can be demonstrated by recent OAIC decisions. For example, in May 2015, Timothy Pilgrim, the Information Commissioner determined the outcome of a complaint by complainant Ben Grubb in relation to access to personal information against Telstra Corporation Limited under s36 of the *Privacy Act*.[44] Similarly another case relating to use and disclosure by a medical practitioner of a patient's medical information and subsequent breaches of National Privacy Principles (*NPP*s) was determined by the Commissioner in March 2015.[45] The outcome of these cases clarify the obligations that industry has in relation to personal privacy collection, use and disclosure protection under the *Privacy Act* and the 'new' *APP*s.

As a consequence of its important role in privacy protection, it is acknowledged that the OAIC provides a robust and independent mechanism by which obligations relating to personal information protection, complaints and industry guidelines under the *Privacy Act* are determined. Nevertheless, the thesis argues that by adding a

[43] See chapter 5, pp174-183.

[44] *Ben Grubb and Telstra Corporation Limited* [2015] AlCmr 35 (1 May 2015) [This case concerned the failing of Telstra to provide the complainant with access to his personal information held by Telstra in breach of National Privacy Principle (NPP) 6.1 of the *Privacy Act 1988* (Cth)]. The determination found in favour of the complainant and clarified 'personal information'.

[45] *'EZ' and 'EY'* [2015] AlCmr 23 (27 March 2015) [this case concerned a complaint against a medical practitioner who released information to police officer].

Council to the privacy rights and protection mix, which supports direct citizen access will positively supplement and enhance rather than diminish or duplicate healthcare information privacy protection oversight in Australia.

As articulated throughout the thesis, a *Council's* purpose is to further localise and strengthen consumer healthcare privacy protection, be a cost effective mechanism that provides an extra layer of public administrative sector transparency and encourage democratic citizen participation.[46] It also aims to exemplify a much needed focus upon citizens as not just receivers of 'goods and services' by economic players and reintroduce 'balance' between all stakeholder interests, by providing a 'forum' in which citizens can voice their concerns be heard and counted. A *Council* will ensure that 'democratic' administrative and institutional values built up over the years in Australia is afforded proper recognition, is 'balanced' and given ongoing protection in the modern knowledge and information economy era.[47] Additionally, the promotion of 'democratic citizenship' will result in better collaboration between public and private authorities and includes:

> [E]ducation, dissemination, information, practices and activities which aim by equipping citizens with knowledge, skills and understanding motivation and behaviour, to empower them to exercise and defend their democratic rights and responsibilities in society, to value

---

[46] See, for example, Council of European Charter on Education for Democratic Citizenship and Human Rights Education, Recommendation CM/Rec (2010) 7 and Explanatory Memorandum, which states: 'Partnership and collaboration should be encouraged among the wide range of stakeholders involved in education for democratic citizenship and human rights at state, regional and local level so as to make the most of their contribution, including policy makers … and the general public': at 10 http://www.coe.int/t/dg4/education/edc/1_What_is_EDC_HRE/What_%20is_en.asp#TopOfPage (viewed on 12/11/2014).

[47] See, Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (April 2013) 11 (5) *Northwestern Journal of Technology and Intellectual Property* 239, the authors argue the role of individual control and data must be in 'usable format' in the 'age of big data'. 'If organizations provide individuals with access to their data in usable formats, creative powers will be unleashed to provide users with applications and features building on their data for new innovative uses': at 272. Additionally, 'traditional transparency and individual access mechanisms have proven to be an ineffective means for motivating individuals to engage their data': at 272.

> diversity and to play an active part in democratic life, with the view to the promotion and protection of democracy and the rule of law.[48]

This *Council* is established under statutory authority, and is required to provide an annual report directly to parliament.[49] It represents a broad range of citizen view with wide powers to hold hearings; access and disseminate information; and liaise with appropriate governing and coordinating bodies. The *Council* model aligns with established Citizen Advisory Boards (*CAB*) and Citizen Advisory Councils (*CAC*) located in Europe, the US and Canada.[50] However, unlike *CAB* or *CAC*, the *Council* is made up of one national forum with direct access to the Minister of Health and the federal Parliament rather than many states and local Community forum coming together. It represents the combined interest (local, territory/state) of a wide range of *PCEHR* and e-health consumers. Similar to *CAB* and *CAC* objectives, the *Council* increases the deliberativeness and overview of government by engaging volunteer citizens and allowing them to become part of the political and government processes that occur in their community. This involvement serves to educate and 'overcome citizen apathy and disinterest by crafting lively and engaging participation programs.'[51]

---

[48] Council of European Charter on Education and Democratic Citizenship and Human Rights Education, above n46.

[49] See, for example, *Ombudsman Act* 1976 (Cth), which outlines the role of the Ombudsman to investigate maladministration in government departments (s 4(2), s 5). The Ombudsman is also required to provide an annual report to parliament. The Ombudsman falls within the Prime Minister's portfolio under the 12 December 2013 Administrative Arrangements Order.

[50] Jason Courter, Citizen Advisory Board (4 June 2010) http://particidedia.net/en/methods/citizen-advisory-board (viewed on 12/8/2015); DC Government, Metropolitan Police Department, Citizens Advisory Councils (CAC) http://mpdc.dc.gov/page/citizens-advisory-councils-cac (viewed on 12/8/2015); Government of Canada, Correctional Service Canada, Citizen Advisory Committees (CAC) http://www.csc-scc.gc.ca/cac/index-eng.shtml (viewed on 12/8/2015).

[51] See Jason Courter, Citizen Advisory Board, above n50, 1.

The Council's responsibilities include but are not limited to 'the study of critical issues, taking public testimony, performing independent research, and reviewing reports and recommendations' of *SCoH* and other committees.[52] These prepare the advisory body to 'discuss, formulate, analyse and forward well-developed, considered recommendations to the legislative body.'[53] It will provide a report of findings and recommendation to be tabled in Parliament. Thus the *Council* is ultimately accountable to Parliament rather than the Health Minister, the Standing Council of Health (*SCoH*), or any other statutory Committee or body. It will be a highly visible forum reinforcing for the community the importance and commitment of democratic open accountable Government processes and community involvement.

Consequently, a *Council* mandate represents a wider view than just 'individual' privacy problems and its mission is more specific than just 'collective decisions' — it represents and fosters local and community involvement. It is recognised that collective political pressure groups such as the Consumer Advocacy Forum, set up to lobby and promote a particular consumer viewpoint may prove inadequate in the modern economic environment, particularly as the number of economic actors increase their power base. Unlike other groups such as the Consumer Advocacy Forum, which function as external political forces that politically advise or lobby Government, a *Council* operates within the formal political power structures of the system and is part of the *PCEHR* administrative political environment. It provides a recognised 'forum' for transparent process of public scrutiny overview, which

[52] Jason Courter, Citizen Advisory Board, above n50.
[53] Ibid.

ultimately benefits all stakeholders and reassures the Australian public that citizen 'voice' and concerns is being considered and acted upon in an era of increasing global expansive and transforming technology and economic opportunities. The overall purpose of a *Council,* then, is to focus on the local and national level of *PCEHR* and e-health system privacy protection advances rather than international impact of electronic privacy reform.

The structure of a *Council* to be capitalised on by the reforms recommended in this thesis is that it operates as part of the official governance: the *PCEHR* and e-health political structure. As suggested, it would be created by an Act of Parliament that outlines its structure, membership, objectives, functions and reporting obligations. After establishing the *Council*, the responsibilities of the *Council* must be clearly defined so that it can focus on the assigned task in order to be as effective as possible. Furthermore, there must be adequate funding and support staff provided in order to assist with the administrative elements of operation of the *Council*. While there are many different ways to organise the membership and day-to-day function of a *Council*, it is important that the group is large enough to have a broad range of ideas while remaining small enough that it is easy to manage. A key feature of the *Council* is its overview and decision-making capacity. It is recommended that the *Council* has both an advisory capacity as well as administrative power to make policy decisions.

Qualifications for appointment are proposed to be open any citizens able to show a legitimate interest and some proven experience in the healthcare and privacy area, drawn from a panel of names nominated by a representative range of consumer health bodies (from peaks to community health centres within the states and

territories). Members do not need to come from a healthcare professional or IT background, in fact this may be discouraged because a *Council* will have the capability in its own right to gather and access experts in any area that it deems relevant as part of its overall function. It is also imperative that members are statutorily empowered to (no gag provisions) and are capable of effectively communicating with the general public, Government and other important stakeholders. As a result it is necessary that members display a high level of communication skill, knowledge and understanding of the problems and solutions needed to progress the debate and represent the interests and viewpoints of multiple healthcare consumers in relation to the governance and privacy debate.

It is envisaged that a representative of the OAIC be appointed as a full member of the *Council* in order to contribute to the debate about resource allocation, privacy guidelines and any other legal mechanisms that already exist in relation to the *PCEHR* and e-health privacy protection in the area. The proposed membership is set at up to 20 representatives, who include: two members from each state and territory, regardless of size, to be determined by each state and territory and chosen by lot (16 members), the rationale for election of members by 'lot' for the *Council* follows the Athenian system (and jury selection method) ensuring that all eligible citizens have equal opportunity (lottery chance) in relation to being elected to the *Council*.[54] With the 'election' of 16 state and territory members (through 'lot'), an OAIC representative appointed by the Information Commissioner and two members of the public and

[54] John Dryzek and Patrick Dunlevy, *Theories of the Democratic State* (Palgrave Macmillan, 2009) In Athens office holders were not elected, but instead selected by lot, to serve for a limited period. This practice has recently been revived in practice associated with deliberative democracy: at 19, 218.

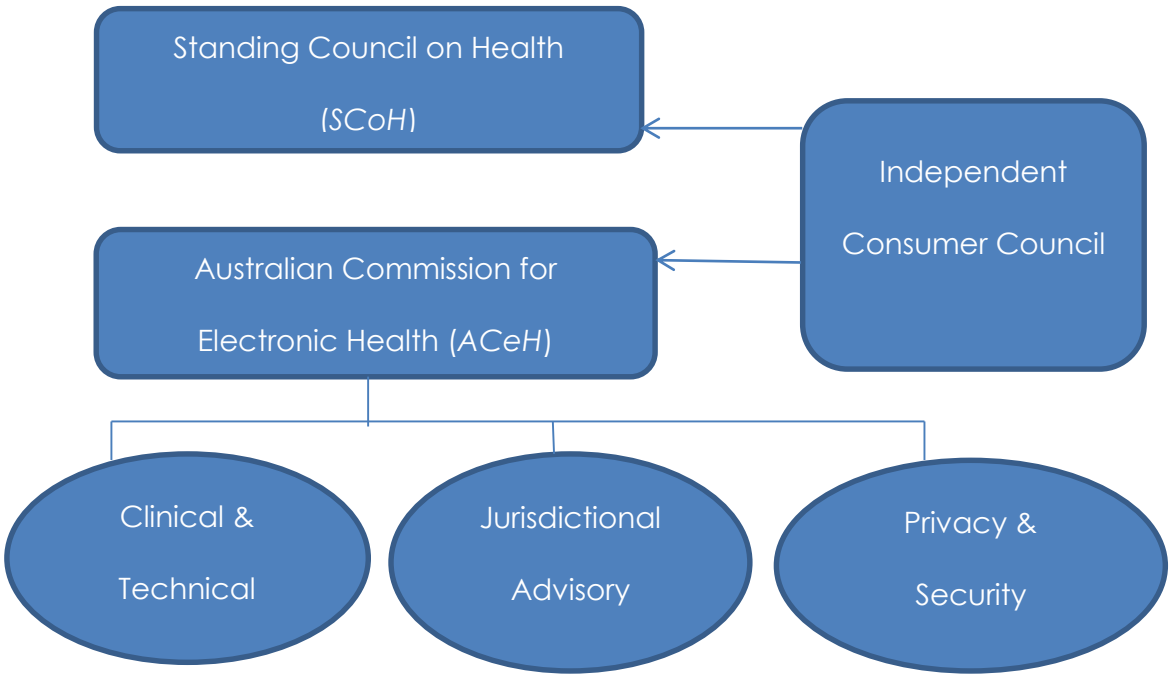
private health sector appointed by the Minister of Health (19 members). All members are appointed for a period of two years. The Chair of the *Council* is counted as a separate member (bringing the total to 20 members) and will be elected by the *Council* members from the general state and territory membership (not the appointed membership) and the position will rotate annually.

This membership number is judged to represent the most efficient balance in regard to a *Council's* objective because too many or too few participating members may not adequately reflect or maximise the best possible outcome of discursive discourse and reporting.[55] Additionally members must demonstrate their capacity to understand the issues that arise in e-health and privacy discourse and act in the interests of citizens rather than come to the forum with preconceived or political partisan ideals or ideas.

Under the proposals advanced in this thesis the Independent Advisory Council established under the *PCEHR Act* and comprising of healthcare professionals and IT experts would become a sub-committee reporting to the Australian Commission for Electronic Health (*ACeH*) and absorbed into the Clinical and Technical Advisory sub-committee. The following is a diagram that represents the proposed thesis governance recommendation structure.

Diagram 2 – **New Governance Structure**:

[55] See, for example, Council of Europe Charter on Education for Democratic Citizenship and Human Rights Education, Recommendation CM/Rec (2010) 7 and Explanatory Memorandum, above n46.



While the main structural arguments suggested by the *Royle Review* about creating an Australian Commission for Electronic Health and the establishment of numerous sub-committees feeding back into *ACeH* are retained by the thesis proposal, the suggested focus and overall structure would shift away from health industry and professional decision-making preference to a more consumer orientated system. A *Council* would be independent of the *ACeH* but able to monitor its activities as well as feed information to the appropriate committee and sub-committees. A *Council* would monitor government, public service and independent bodies *PCEHR* and e-health system governance role; inform the public and give considered advice about consumer concerns and interests. Decision-making directly affecting *PCEHR* and e-health privacy by the *ACeH* including oversight of current and future policies would require oversight by a *Council* before adoption. In most circumstances it is anticipated

that this would not be an overly complicated nor duplicative process. It would work in conjunction with other statutory bodies such as the Information Commissioner to ensure that these bodies are sufficiently resourced by Government in order to carry out their particular role. As mentioned, a *Council* would be properly resourced and have access to relevant information and experts in the area under consideration. It would report as required to the Standing Council on Health, the Health Minister as well as Parliament.

III. THESIS CONCLUSION

With the ultimate convergence of computers and communication technology it emerges that, as a society, Australians will be likely stepping into a future that is unknown and to some degree unpredictable. However, this uncertainty of the future does not mean that one should not consider, contest, question or indeed cease to have an active role in how the future Government or governance mechanisms are eventually organised. Believing that the intrusive adoption of technology advances is the only viable option available for people and that its unfettered progress is inevitable potentially disempowers an individual's ability to contribute in a positive way to their community. The provision of health and healthcare services in Australia, as well as how privacy is conceived including how our personal sensitive health information is collected, stored and disclosed in an increasingly 'sharing' and 'networking' society and the issue of diminishing democratic privacy protection rights remains an

important consideration and must be vigorously protected now and in the future for all the reasons set out in the previous chapters.[56]

This thesis has argued that privacy and ongoing healthcare privacy protection remains an important consideration for society, individuals and the community and that changing our approach to how this will be understood and organised now and in the future should not be left to chance or be about capitalism and economic profit generation. The blurring of lines between private and public, between political and economic distinctions, are being constantly challenged and eroded by rapid advancing technology and globalisation interests to the detriment of democratic values and processes. This situation deserves serious citizen attention and increased active commitment by people power as citizens morally and legally 'grapple' with these changes in the modern information economy. The various chapters in this thesis have highlighted the multi-dimensional aspects of modern era health, technology and privacy in Australia. It has also organised this information by analysing the approach suggested by successive Australian Governments over the last few decades – the trilogy of legislation, technical and governance measures. The chapters have argued that despite the best efforts by previous Governments to expedite and obtain economic value from the e-health program that we may need to consider a radically different approach, which combines a more 'balanced' collective and individual interest approach by all stakeholders to the healthcare privacy debate (consumers, industry and professional groups). It is also argued in the thesis that the concept of privacy is

[56] See Martha Nussbaum, *Not for Profit: Why Democracy Needs the Humanities* (Princeton University Press, 2010). Nussbaum outlines the importance of 'Socratic Pedagogy: The Importance of Argument' to preserve transparency and accountability: at 47.

far more complex in the modern age than just relegating it to data information collection, use and disclosure – making it necessary to view privacy as an important value attached to broader human rights issues such as democracy.[57]

Additionally, the thesis highlights the proposition that, because consumers stand to lose the most 'rights' by adopting the *PCEHR* and e-health system, they should become the political priority in relation to future decision-making activities. While the health profession and industry is important to support and promote the new system it must be viewed as just one important component; and as a consequence its interests should be protected and encouraged but not preferred or prioritised. Further it is contended that the introduction of a *Council* will provide a significant move towards promoting citizen 'ownership' and participation of the new electronic healthcare regime. The thesis sets out the main arguments for why a *Council* needs to be considered and introduced as a highly desirable and viable option of promoting democratic citizen participation in the *PCEHR* and e-health system in Australia. As a consequence, it is maintained that if privacy is an important human right worth protecting against economic and political exploitation then it stands to reason that it must be vigorously defended against the threat of individual complacency and compliance as we continue to engage in the new technological era.

[57] See, Australian Law Reform Commission (ALRC), *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws*: Issues Paper 46 (December 2014). The terms of reference for IS 46 emerges from a number of modern day concerns relating to rights and freedoms such as freedom of speech, procedural fairness to persons affected by the exercise of public power. It also identifies Commonwealth laws that encroach upon traditional rights, freedoms and privileges; and a critical examination of those laws to determine whether the encroachment upon those traditional rights, freedoms and privileges is appropriately justified: at 1, 5-7.

BIBLIOGRAPHY

A. BOOKS

Agre, Philip and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001)

Akindemowa, Olujoke, *Information Technology Law in Australia* (Thomas Reuters, 1999)

Allan, Sonia and Meredith Blake, *The Patient and the Practitioner: Health Law and Ethics in Australia* (LexisNexis, 2014)

Allen, Anita, *Uneasy Access: Privacy for Women in a Free Society* (Allen Rowman & Littlefields Publication, 1988)

Allott, Philip, *The Health of Nations: Society and Law Beyond the State* (Cambridge University Press, 2002)

Angell, Marcia, *The Truth About the Drug Companies* (Random House, 2005)

Arendt, Hannah, *The Human Condition* (University of Chicago Press, 1958)

Arup, Christopher, *Innovation, Policy and Law: Australia and the International High Technology Economy* (Cambridge University Press, 1993)

Astor, Hilary and Christine Chinkin, *Dispute Resolution in Australia* (LexisNexis, 2nd ed, 2002)

Australian Institute of Health and Ethics (eds), *Public Health in Australia: New Perspectives* ([Canberra]: The Institute, 1998)

Ayers, Ian and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992)

Ballard, Edward, *Man and Technology: Towards the Measurement of a Culture* (Duquesne University Press, 1978)

Baier K and N Rescher (eds), *Values and the Future* (Free Press, 1969)

Beauchamp, Tom and James Childress, *Principles of Biomedical Ethics* (Oxford University Press, 4th ed, 1994)

Benn, S and G Gaus (eds), *Public and Private in Social Life* (St Martin's Press, 1983)

Bennett, Belinda, *Law and Medicine* (LBC Information Services, 1997)

Bennett, Belinda, Terry Carney and Isabel Karpin (eds), *Brave New World of Health* (The Federation Press, 2008)

Berlin, Isaiah Sir, *Four Essays on Liberty* (Clarendon Press, 1958)

Berryman, Jeffrey and Rick Bigwood (eds), *The Law of Remedies: New Directions in the Common Law* (Irwin Law, 2010).

Beverely-Smith, Huw, *The Commercial Appropriation of Personality* (Cambridge University Press, 2008)

Biegel, Stuart, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press, 2003)

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

Bok, Sissela, *Secrets: On the Ethics of Concealment and Revelation* (Random House, 1983)

Borgmann, Albert, *Technology and the Character of Contemporary Life* (University of Chicago Press, 1987))

Bowrey, Kathy, *Law and Internet Culture* (Cambridge University Press, 2005)

Burns, Lawton Robert (ed), *The Business of Healthcare Innovation* (Cambridge University Press, 2005)

Butler, Des and Sharon Rodrick, *Australian Media Law* (Thomas Reuters, 4th ed, 2011)

Braithwaite, John, *Regulatory Capitalism* (Edward Elger, 2008)

Braithwaite, John and P Drahos, *Global Business Regulations* (Cambridge University Press, 2000)

Brin, David, *The Transparent Society* (Perseus Books, 1998)

Brown, Marvin, *Corporate Integrity: Rethinking Organisational Ethics and Leadership* (Cambridge University Press, 2005)

Caldwell, John, Sally Findley, Pat Caldwell and Gigi Santow, Wendy Cosford, Jennifer Braid and Dalhne Broers-Freemen (eds), *What We Know About Health Transition: The Cultural, Social and Behavioural Determinants of Health* (Health Transition Series No 2, 2001)

Carney, Gerard, *The Constitutional Systems of the Australian States and Territories* (Cambridge University Press, 2006)

Cassese, Antonio, *International Law* (Oxford University Press, 2001)

Chalmers, Alan, *What is this Thing Called Science?* (University of Queensland Press, 3rd ed, 1999)

Clarke, Bruce, Brendan Sweeney and Mark Bender, *Marketing and the Law* (LexisNexis, 4th ed, 2011)

Clarke, Jennifer, Patrick Keyzer, James Stellios and John Trone, *Hanks Australian Constitutional Law: Material and Commentary* (LexisNexis, 9th ed, 2012).

Corones, S G, *The Australian Consumer Law* (Routledge-Cavendish, 2011)

Cotterrell, Roger, *The Politics of Jurisprudence* (Butterworths, 1989)

Couvalis, George, *Philosophy of Science: Science and Objectivity* (Sage Publications, 1997)

Coyne, Richard, *Designing Information Technology in the Postmodern Age: From Methods to Metaphor* (The MIT Press, 1995)

Crane, Andrew and Dirk Matten, *Business Ethics* (Oxford University Press, 3rd ed, 2010)

Creyke, Robin and John McMillan, *Control of Government Action* (LexisNexis, 3rd ed, 2012)

Creighton, Breen and Andrew Stewart, *Labour Law* (The Federation Press, 2010)

Davidson, Alan, *The Law of Electronic Commerce* (Cambridge University Press, 2nd ed, 2012)

DeCrew, Judith Wagner, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Cornell University Press, 1997)

Devereux, John, *Australian Medical Law* (Routledge-Cavendish, 3rd ed, 2007)

Diego, Gambetto (ed), *Trust: Making and Breaking Cooperative Relations* (Oxford University Press, 2000)

Dixon, Martin, Robert McCorquodale and Sarah Williams, *International Law* (Oxford University Press, 5th ed, 2011)

Douglas, Roger, *Administrative Law* (LexisNexis, 2nd ed, 2004)

Doyle, Carolyn and Mirko Bagaric, *Privacy Law in Australia* (The Federation Press, 2005)

Duffy, Helen, *The 'War on Terror' and the Framework of International Law* (Cambridge University Press, 2005)

Dunphy, Dexter, Andrew Griffiths and Suzanne Benn, *Organisational Change for Corporate Sustainability* (Routledge, 2003)

Dryzek, John and Patrick Dunleavy, *Theories of the Democratic State* (Palgrave Macmillan, 2009)

Ellul, Jacques, *The Technological Society* (Vintage Press, 1964)

Etzioni, Amitai, *The Limits of Privacy* (Basic Books, 1999)

Etzioni, Amitia, *The Spirit of Community* (Touchstone Books, 1994)

Farrar, John, *Corporate Governance* (Oxford University Press, 2nd ed, 2006)

Feenberg, Andrew, *Transforming Technology: A Critical Theory Revisited* (books.google.com. 2002)

Feenberg, Andrew, *Critical Theory of Technology* (Oxford University Press, 1991)

Fenwick, Colin and Tonia Novitz (eds), *Human Rights at Work* (Onati International Series in Law and Society, 2010)

Ferre, Fredrick, *Philosophy of Technology* (University of Georgia Press, 1995)

Flynn, Martin, Sam Garkawe and Yvette Holt, *Human Rights Treaties, Statutes and Cases* (LexisNexis, 2011)

Fisher, Colin and Alan Lovell, *Business Ethics and Values* (Prentice Hall, 3rd ed, 2009)

Fitzgerald, Brian and Anne Fitzgerald, *Cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property, and Electronic Commerce* (LexisNexis, 2002)

Fitzgerald, Brian, Anne Fitzgerald, Eugene Clark, Gaye Middleton and Yee Fen Yim, *Internet and E-Commerce Law* (Routledge-Cavendish, 2011)

Forrester, Kim and Debra Griffiths, *Essentials of Law for Health Professionals* (Elsevier, 2009)

Freckelton, Ian and Kerry Petersen (eds), *Disputes and Dilemmas in Health Law* (The Federation Press, 2006)

Freed, Les and Sarah Ishida, *History of Computers* (Ziff-Davis Publishers, 1995)

Friedman, Batya (ed), *Human Values and the Design of Computer Technology* (Cambridge University Press, 1997)

Galligan, Brian, Winsome Roberts and Gabrielle Trifiletti, *Australians and Globalisation: The Experience of Two Centuries* (Cambridge University Press, 2001)

Gamertsfelder, Leif, *E-Security* (Thomas-Reuters, 2002)

Gardner, Heather and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2002)

Gaze, Beth and Melinda Jones, *Law, Liberty and Australian Democracy* (The Law Book Company Limited, 1990)

Goodman, Kenneth (ed), *Ethics, Computing and Medicine* (Oxford University Press, 1998)

Goldsmith, Edward and Jerry Mander (eds), *The Case Against the Global Economy* (Earthscan Publication, 2001)

Giles, Roslyn, Irwin Epstein and Anne Vertigan (eds), *Clinical Data-Mining in an Allied Health Organisation* (Sydney University Press, 2011)

Grace, Damian and Stephen Cohen, *Business Ethics* (Oxford University Press, 4th ed, 2010)

Gray, J. A. Muir, *Evidence-based Healthcare* (Churchill Livingstone, 1997)

Grasbosky, Peter, Russell Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press, 2001)

Groves, Matthew and H. P. Lee (eds), *Australian Administrative Law* (Cambridge University Press, 2007)

Grubb, Andrew, Judith Lang and Jean McHale, *Principles of Medical Law* (Oxford University Press, 3rd ed, 2010)

Haas, Michael, *International Human Rights* (Routledge, 2008)

Habermas, Jurgen, *The Postnational Constellation* (Cambridge University Press, 2001)

Habermas, Jurgen (ed), *The Inclusion of the Other: Studies in Political Theory* (The MIT Press, 1998)

Habermas, Jurgen, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (The MIT Press, 1989)

Hamilton, Clive and Sarah Maddison, *Silencing Dissent* (Allen and Unwin, 2007)

Hanks, P J, *Constitutional Law in Australia* (Butterworths, 1991)

Handl, G, J Zekoll and P Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalisation* (Martin Nihhoff Publisher, 2012)

Heidegger, Martin, *The Question Concerning Technology* (Harper and Row Publishers, 1977)

Hobart, Michael and Zachary Schiffman, *Information Ages: Literacy, Numeracy and the Computer Revolution* (Johns Hopkins University Press, 2000)

Huxley, Aldous, *1984* (Penguin Books, 1949)

Ihde, Don, *Heidegger's Technologies: Post Phenomenological Perspectives* (Fordham University Press, 2010)

Ihde, Don, *Philosophy of Technology* (Paragon House, 1993)

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

Jackson, Peter, Michelle Lowe, Daniel Miller and Frank Mort (eds), *Commercial Cultures* (Berg Publications, 2000)

Johnstone, Megan-Jane, *Bioethics (*Harcourt Brace, 2nd ed, 1994)

Johnstone, Megan-Jane, *Nursing and the Injustices of the Law* (Hardcastle Brace & Co, 1994)

Kellner, Douglas, *Critical Theory, Marxism, and Modernity* (Polity Press, 1989)

Kelly, MRLL, *Administrative Law* (Thomas Reuters, 2015)

Kennedy, Ian and Ian Grubb (eds), *Medical Law: Text and Material* (Oxford University Press, 1998)

Katz, Jay, *The Silent World of Doctors and Patient* (John Hopkins University Press, 1984)

Keel, Peter and Normal Lucas, *Reputation Matters* (CCH Australia, 2007)

Keleher, Helen and Colin MacDougall (eds), *Understanding Health* (Oxford University Press, 2nd ed, 2012)

Kenyon, Andrew and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006)

Kerridge, Ian, Christopher Jordens and Emma-Jane Sayers (eds), *Restoring Human Values to Medicine* (Desert Pea Press, 2003)

Klang, Mathias and Andrew Murray (eds), *Human Rights in the Digital Age*, (Routledge-Cavendish, 2005)

Kuhn, Thomas, *The Structure of Scientific Revolution* (University of Chicago Press, 1962)

La Nauze, J A, *Federated Australia: Selections from Letters to the Morning Post 1900-1910* (Melbourne University Press, 1968)

Lane, Frederick, *The Naked Employee* (Amacom, 2003)

Lanier, Jaron, *Who Owns the Future* (Penguin Books, 2013)

Lanier, Jaron, *You Are Not a Gadget: A Manifesto* (Alfred A Knopf, 2010)

Laurie, Graeme, *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, 2002)

Locke, Robert and J-C Spender, *Confronting Managerialism* (Zed Books, 2011)

Lewis, Jenny, *Health Policy and Politics: Networks, Ideas and Power* (IP Communications Melbourne, 2005)

Luhmann, Niklas, *Social Systems* (books.google.com. 1995)

Lumb, R D and K W Ryan, *Constitution of Australia* (Butterworth, 1977)

Luntz, Harold and David Hambly, *Torts: Cases and Commentary* (LexisNexis, 7th ed, 2011)

Marcus, Herbert, *One Dimensional Man* (Beacon Books, 1968)

Mason, Brett, *Privacy Without Principle* (Australian Scholarly Publishing, 2006)

Masum, Hassan and Mark Toovey (eds), *The Reputation Society: How Online Opinions are Shaping the Offline World* (The MIT Press, 2011)

Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009)

Maynard, Alan (ed), *The Public-Private Mix for Health* (Radcliffe Publication, 2005)

MacIntyre, Clement and John Williams (eds), *Peace, Order and Good Government* (Wakefield Press, 2003)

McGrath, Frank, *The Framers of the Australian Consititution 1891-1897: Their Intentions* (Frank McGrath, 2003)

McIlwraith, Janine and Bill Madden, *Health Care and the Law* (Thomas Reuters, 6th ed, 2014)

McNeill, Paul, *The Ethics and Politics of Human Experimentation* (University of Cambridge Publication, 1993)

Madden, Bill and Janine McIlwraith, *Australian Medical Liability* (LexisNexis, 2013)

Medhurst, Robert, *The Business of Healing* (Hyde Park Press, 2002)

Morgan, Derek, *Issues in Medical Law and Ethics* (Cavendish Press, 2001)

Morozov, Evengy, *To Save Everything Click Here: The Folly of Technological Solutionism* (Penguin Books, 2013)

Morozov, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom* (Penguin Books, 2012)

Morozov, Evengy, *The Net Delusion: How Not to Liberate the World* (books.google.com. 2011)

Nissenbaum, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, 2010)

Nussbaum, Martha, *Not for Profit: Why Democracy Needs the Humanities* (Princeton University Press, 2010)

Owens, Rosemary, Joellen Riley and Jill Murray, *The Law of Work* (Oxford University Press, 2nd ed, 2011)

Painter, Martin, *Collaborative Federalism: Economic Reform in Australia in the 1990s* (Cambridge University Press, 1998)

Palmer, George and Stephanie Short, *Health Care and Public Policy* (Palgrave Macmillan Publication, 4th ed, 2011)

Parkinson, John, *Deliberating in the Real World: Problem of Legitimacy in Deliberative Democracy* (Oxford University Press, 2006)

Parrenas, Salazar Rhacel, *Servants of Globalisation: Women, Migration and Domestic Work* (Stanford University Press, 2001)

Paterson, Moira, *Freedom of Information and Privacy in Australia* (LexisNexis, 2005)

Pawson, Ray, *Evidence-Based Policy* (Sage Publication, 2006)

Pennock, Roland and J Chapman (eds), *Nomas XIII: Privacy* (Roland Pennock & J Chapman, 1971)

Pharr, Susan and Robert Putnam (eds), *Disaffected Democracies* (Princeton University Press, 2000)

Popper, Karl, *The Logic of Scientific Discovery* (Routledge, 1959)

Porter, Roy, *The Greatest Benefit to Mankind: A Medical History of Humanity from Antiquity to the Present* (Harper Collins Press, 1997)

Postman, Neil, *Technopoly* (Vintage Books, 1993)

Posner, Richard, *Economics of Justice* (Harvard University Press, 1981)

Rapp, Friedrich, *Analytical Philosophy of Technology* (Cambridge University Press, 1989)

Regan, P, *Legislating Privacy* (University of North Carolina Press, 1995)

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

Rosen, Jeffrey, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books, 2001)

Richards, Bernadette and Jennie Louise, *Medical Law and Ethics A Problem-Based Approach* (LexisNexis, 2014)

Rule, James, *Privacy in Peril* (Oxford University Press, 2007)

Sarre, Rick and Tim Prenzler, *The Law of Private Security in Australia* (Thomson Reuters, 2nd ed, 2009)

Sawer, Geoffrey, *Federation Under Strain: Australia 1972-1965* (Melbourne University Press, 1977)

Schmidt, Eric and Jared Cohen, *The New Digital Age* (John Murray, 2013)

Schoeman, Ferdinand (ed), *Philosophical Dimensions of Privacy: An Anthology* (F D Schoeman, books.google.com. 1984)

Sen, Amartya, *The Idea of Justice* (Harvard University Press, 2009)

Skene, Loane, *Law and Medical Practice* (LexisNexis, 3rd ed 2008)

Simons, Penelope and Audrey Macklin, *The Governance Gap* (Routledge, 2014)

Smith, Russell, Peter Grabosky and Gregor Urbas, *Cyber Criminals on Trial* (Cambridge University Press, 2004)

Solove, Daniel, Marc Rotenberg and Paul Schwartz, *Privacy, Information, and Technology* (Aspen Publication, 2006)

Solove, Daniel, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011)

Solove, Daniel, *Privacy, Information and Technology* (Aspen Publication, 2006)

Solove, Daniel, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004)

Solove, Daniel, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, 2007)

Solove, Daniel, *Understanding Privacy* (Harvard University Press, 2010)

Stanworth, Michael (ed), *Reproductive Technologies: Gender, Motherhood and Medicine* (Polity Press, 1987)

Stewart, Andrew, *Employment Law* (The Federation Press, 5th ed, 2015)

Subramanian, Ramesh and Eddan Katz (eds), *The Global Flow of Information: Legal, Social, and Cultural Perspectives* (New York University Press, 2011)

Stone, Richard, *Civil Liberties & Human Rights* (Oxford University Press, 8th ed, 2010)

Tallis, Raymond, *Hippocratic Oaths: Medicine and its Discontent* (Atlantic Books, 2004)

Taylor, Sandra, Michele Foster and Jennifer Fleming (eds), *Health Care Practice in Australia* (Oxford University Press, 2008)

Tang, Cheryl, *Microsoft First Generation* (John Wiley & Sons, 2000)

Teubner, G (ed), *Autopoietic: A New Approach to Law and Society* (Walter de Gruyter, 1988)

Teubner, G (ed), *Juridification of Social Spheres* (Walter de Gruyter, 1987)

Van Dijk, Jan, *The Network Society* (Sage Publication, 2012)

Van Dijk, Jan, *The Deepening Divide: Inequality in the Information Society* (books.google.com. 2005)

Wajcman, Judy, *Feminism Confronts Technology* (Allen & Unwin, 1991)

Webster, Frank, *Theories of the Information Society* (Routledge-Cavendish, 2002)

Weir, Michael, *Law and Ethics in Complementary Medicine* (Allen and Unwin, 4th ed, 2011)

Westin, Allan, *Privacy and Freedom* (Bodley Head, 1967)

Whetton, Sue, *Health Informatics: A Socio-Technical Perspective* (Oxford University Press, 2005)

White, Ben, Fiona McDonald and Lindy Willmott, *Health Law in Australia* (Thomas Reuters, 2nd ed, 2014)

Willis, Eileen, Louise Reynolds and Helen Keleher (eds), *Understanding the Australian Health Care System* (Elsevier, 2012)

Williams, George, *A Bill of Rights for Australia* (New South Publishing, 2000)

Williams, George, *Human Rights under the Australian Constitution* (Oxford University Press, 1999)

Williams, George, Sean Brennan and Andrew Lynch, *Blackshield & Williams Australian Constitutional Law & Theory* (The Federation Press, 6th ed, 2012)

Winner, Langdon, *Autonomous Technology: Technics-Out-Of-Control as a Theme in Political Thought* (The MIT Press, 1977)

Zetler, Julie and Rodney Bonello, *Essentials of Law, Ethics and Professional Issues* (Elsevier, 2012)

B BOOK CHAPTERS

Abbott, Fredrick, 'Emerging Market Pharmaceutical Supply: A Prescription for Sharing the Benefits of Global Information Flow' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 175

Agre Philip, 'Beyond the Mirror World: Privacy and the Representational Practices of Computing' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001) 29

Backer, Larry Cata, 'Governance without Government: An Overview' in G Handl, J Zekoll and P Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalisation* (Martin Nihhoff Publisher, 2012) 118

Balkin, Jack, 'Information Power' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 232

Balkin, Jack, 'Information Power: The Information Society from an Antihumanist Perspective' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 232

Barlow, John Perry, 'A Declaration of the Independence of Cyberspace' in Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press, 2nd ed, 2012) 14

Benn, Stanley, 'Privacy, Freedom and Respect for Persons' in J R Pennock and J W Chapman (eds), *Nomas XIII: Privacy* (Armonk Publications, 1971)

Bennett, Belinda, 'Globalising Rights? Constructing Health Rights in a Shrinking World' in Belinda Bennett, Terry Carney and Isabel Karpin (eds), *Brave New World of Health* (The Federation Press, 2008) 8

Berlin, Isaiah Sir, 'Two Concepts of Liberty' in Sir Isaiah Berlin, *Four Essays on Liberty* (Clarendon Press, 1958) 4

Bertrand, Agnes and Laurence Kalafatides, 'The World Trade Organisation and the Liberation of Trade in Healthcare and Services' in Edward Goldsmith and Jerry Mander (eds), *The Case Against the Global Economy* (Earthscan Publication, 2001) 217

Brownsword, Roger, 'Biotechnology and Rights: Where are we Coming From and Where are we Going?' in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Routledge-Cavendish, 2005) 219

Carey, Michael and Merilyn Walton, 'On Trust' in Ian Kerridge, Christopher Jordens and Emma-Jane Sayers (eds), *Restoring Human Values to Medicine* (Desert Pea Press, 2003) 166

Carney, Terry, 'Human Rights and Health Law' in Ben White, Fiona McDonald and Lindy Willmott (eds), *Health Law in Australia* (Thomas Reuters, 2nd ed, 2014) 114

Davies, Simon, 'Re-Engineering Rights to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (The MIT Press, 2001) 143

Das, Veena, 'What Do We Mean by Health?' in John Caldwell, Sally Findley, Pat Caldwell, Gigi Santow, Wendy Cosford, Jennifier Braid and Dalhne Broers-Freeman (eds), *What We Know About Health Transition: The Cultural, Social and Behavioural Determinants of Health* (Health Transition Series No. 2, 2001) 16

Denning, Dorothy, 'Power Over Information Flow' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 218

Drezner, Daniel, 'Weighing the Scales: The Internet's Effect on State-Society Relations' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 121

Freund, Paul, 'Address at the American Law Institute' (Address to 52nd Annual American Law Institute Meeting, 1975)

Garrard, Jan, 'Evidence and Public Health: Data, Discourse, and Debates' in Helen Keleher, Colin MacDougall (eds), *Understanding Health* (Oxford University Press, 2nd ed, 2012) 59

Goodman, Kenneth, 'Outcomes, Futility, and Health Policy Research' in Kenneth Goodman (ed), *Ethics, Computing and Medicine* (Oxford University Press, 1998) 129

Grbich, Carol, 'Moving Away from the Welfare State: The Privatisation of the Health System' in Health Gardiner and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2001) 79

Greenleaf, Graham, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press, 2006) 91

Groves, Matthew and H P Lee, 'Australian Administrative Law: The Constitutional Matrix' in Matthew Groves and H P Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007) 1

Habermas, Jurgen, 'Three Normative Models of Democracy' in Jurgen Habermas (ed), *The Inclusion of the Other: Studies in Political Theory* (Cambridge MIT University Press, 1998)

Hancock, Linda, 'Australian Federalism, Politics and Health' in Health Gardiner and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2002) 49

Hardin, Russell, 'The Public Trust' in Susan Pharr and Robert Putnam (eds), *Disaffected Democracies* (Princeton University Press, 2000) 52

Katz, Stanley, 'Prospects for a Global Networked Cultural Heritage: Law Versus Technology?' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 90

Luhmann, Niklas, 'Familiarity, Confidence, Trust: Problems and Alternatives' in Gambetto Diego (ed), *Trust: Making and Breaking Cooperative Relations* (Oxford University Press, 2000) 94

Mander, Jerry, 'Technologies of Globalization' in Edward Goldsmith and Jerry Mander (eds), *The Case Against the Global Economy* (Earthscan Publication, 2001) 45

Mansell, Robin, 'Introduction-Human Rights and Equity in Cyberspace' in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Routledge-Cavendish, 2006) 1

McMillan, John, 'Commonwealth Constitutional Power in Public Health' in Australia Institute of Health Law and Ethics (eds), *Public Health in Australia: New Perspectives* ([Canberra]: The Institute, 1998) 30

Mendelson, Danuta and Anne Rees, 'Confidentiality, Privacy and Access to Health Records' in Ben White, Fiona McDonald and Lindy Willmott (eds), *Health Law in Australia* (Thomas Reuters, 2nd ed, 2014) 301

Mendelson, Danuta and Moira Paterson, 'Privacy Issues, Health Connect and Beyond' in Ian Freckelton and Kerry Petersen (eds), *Disputes and Dilemmas in Health Law* (The Federation Press, 2006) 604

Michaelson, Christopher, 'Antiterrorism Legislation in Australia: A Proportionate Response to Terrorist Threat?' in *Studies in Conflict and Terrorism* (Routledge, 2005)

Mitchell, William, 'City of Bits: Space, Place, and the Infobahn', in Stuart Biegal, *Beyond Our Control* (The MIT Press, 2003) 187

Morris, David, 'Free Trade: The Great Destroyers' in Edward Goldsmith and Jerry Mander (eds), *The Case Against the Global Economy* (Earthscan Publication, 2001) 115

Murchison, Brian, 'Revisiting the American Action for Public Disclosure of Private Facts' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press, 2006) 32

Murray, Andrew, 'Should States Have a Right to Information Privacy?' in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Routledge-Cavendish, 2005) 15

Newton, Kenneth and Pippa Norris, 'Confidence in Public Institutions: Faith, Culture, or Performance?' in Susan Pharr and Robert Putnam (eds), *Disaffected Democracies* (Princeton University Press, 2000) 3

Nussbaum, Martha, 'Educating Citizens' in Martha Nussbaum, *Not for Profit* (Princeton University Press, 2010) 27.

Palombo, Angela, 'Record Creation and Access: The Impact of Legislative Changes' in Ian Freckelton and Kerry Petersen (eds), *Disputes & Dilemmas in Health Law* (The Federation Press, 2006) 63

Perritt, H, 'Jurisdiction in Cyberspace: The Role of the Intermediaries' in Brian Fitzgerald and Anne Fitzgerald, *Cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property, and Electronic Commerce* (LexisNexis, 2002) 122

Rachel, James, 'Why is Privacy Important?' in Ferdinand Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (F D Schoeman, books.google.com. 1984)

Reiman, Jeffrey, 'Privacy, Intimacy and Personhood' in Ferdinand Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (F D Schoeman, books.google.com. 1984)

Rescher, Nicholas, 'What is Value Change? A Framework for Research' in K Baier and N Rescher (eds), *Value and the Future* (Free Press, 1969) 48

Reyes, Victoria and Miguel Angel Centeno, 'McDonald's, Wienerwald, and the Corner Deli' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 23

Roberts, Rosemary, Kerrin Robertson and Dianne Williamson, 'Health Information Policy' in Health Gardner and Simon Barraclough (eds), *Health Policy in Australia* (Oxford University Press, 2nd ed, 2002) 100

Rosen, Jeffrey, 'The Naked Crowd: Balancing Privacy and Security in the Age of Terror' (Paper Presented at Twenty-Fourth Annual Isaac Marks Memorial Lecture on 4 March 2004, Philadelphia)

Samarajiva, Rohan, 'Interactivity As Though Privacy Mattered' in Philip Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (The MIT Press, 2001) 277

Sammut, Stephen, 'Biotechnology Business and Revenue Models: The Dynamic of Technological Evolution and Capital Market Ingenuity' in Lawton Robert Burns (ed), *The Business of Healthcare Innovation* (Cambridge University Press, 2005) 7

Saul, Ben, 'Australian Administrative Law: The Human Rights Dimension' in Matthew Groves and H P Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2007) 50

Saul, Ben, 'Australian Administrative Law' in Matthew Groves and H P Lee (eds), *Australian Administrative Law: Fundamentals, Principles and Doctrines* (Cambridge University Press, 2005) 55

Simons, Penelope, 'The Governance Gap: Multistakeholders and Intergovernmental Initiatives' in Penelope Simons and Audrey Macklin, *The Governance Gap* (Routledge, 2014) 79

Simons, Penelope, 'Private Law Beyond the State: Harder Than Hard Law' in Penelope Simons and Audrey Macklin, *The Governance Gap* (Routledge, 2014) 88

Subramanian, Ramesh and Eddan Katz, 'Perspectives on the Global Flow of Information' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press, 2011) 5

Taylor, Sandra, 'The Concept of Health' in Sandra Taylor, Michele Foster and Jennifer Fleming (eds), *Health Care Practice in Australia* (Oxford University Press, 2008)

Teubner, G, 'Justification – Concepts, Aspects, Limits, Solutions' in G Teubner (ed), *Juridification of Social Spheres* (Walter de Gruyter, 1987)

Teuber, G, 'Introduction to Autopoietic Law' in G Teubner, *Autopoietic: A New Approach to Law and Society* (Walter de Gruyter, 1988) 1

Thomson, Judith Jarvis, 'The Right to Privacy' in *Philosophical Dimensions of Privacy: An Anthology* (F D Schoeman, books.google.com. 1984)

van Dijk, Jan and Kenneth Hacker, 'The Digital Divide as a Complex and Dynamic Phenomenon' in Jan van Dijk, *The Information Society* (Taylor & Francis, 2003) 20

Van den Haag, 'On Privacy' in Roland Pennock and J Chapman (eds), *Nomos XIII: Privacy* (Roland Pennock & J Chapman, 1971) 50

Wilson, Beth, 'Health Systems, Quality Control and Corporatisation: New Challenges for Accountability' in Ian Freckelton and Kerry Petersen (eds), *Disputes & Dilemmas in Health Law* (The Federation Press, 2006) 516

C JOURNALS/PAPERS

Abrams, Martin, 'Privacy, Security and Economic Growth in an Emerging Digital Economy' (Paper presented at Privacy Symposium, Institute of Law China Academy of Social Sciences, 7 June 2006, 18)

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

Alston, Andrew, "Lawyers and Doctors: Entitlement to Breach Confidentiality" (2006) 9(1) *Flinders Journal of Law Reform* 63

Appelbaum, Paul, "Confidentiality in the Forensic Evaluation" (1984) 7 *International Journal of Law and Psychiatry* 285

Appelbaum, Paul, "Threats to the Confidentiality of Medical Records – No Place to Hide" (2000) 283(6) *Journal of the American Medical Association* 795

Au, Richard and Peter Croll, 'Consumer-Centric and Privacy-Preserving Identity Management for Distributed E-Health Systems' (Paper Presented to 41st Hawaii International Conference on Systems Sciences, March 2008)

Backer, L C, "Rights and Accountability in Development ('Raid') v Das Air and Global Witness v Afrimex: Small Steps towards an Autonomous Transnational Legal System for the Regulation of Multinational Corporation" (2009) 10 *Melbourne Journal of International Law* 258

Backstarnd, Karl, "Multi-Stakeholder Partnerships for Sustainable Development: Rethinking Legitimacy, Accountability and Efficiency" (2006) 16 *European Environment* 291

Baran, Paul, "The Future of Computer Utility" (1967) 8 *The Public Interest Policy*

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

Bennett Moses, Lyria, "Recurring Dilemmas: The Law's Race to Keep Up with Technological Change" (2007) 7 *University of Illinois Journal of Law, Technology and Policy* 239

Black, Julia, "Proceduralising Regulation: Part 1" (2000) 20(4) *Oxford Journal of Legal Studies* 597

Black, Julia, "Constitutionalising Self-Regulation" (1996) 59 *The Modern Law Review* 24

Black, Julia, 'Critical Reflections on Regulations' (Paper Presented at Australian Society of Legal Philosophy Conference in Canberra, February 2001); (2002) 27 *Austl.J.Leg.Phil* 1

Bloustein, Edward, "Human Dignity: An Answer to Dean Prosser" (1964) 39 *New York Law Review* 962

Bloustein, Edward, "Privacy as an Aspect of Human Dignity" (1964) 39 *New York University Law Review* 156

Braithwaite, John, "The Essence of Responsive Regulation" (2011) 44 *UBC Law Review* 476

Braithwaite, John, "Responsive Regulation and Developing Economies" (2006) 34(5) *World Development* 884 doi:10.1016/j.worlddev.2005.04.021

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

Burns, Peter, "The Law and Privacy: The Canadian Experience" (1976) 54(1) *Canadian Bar Review* 12

Bygrave, Lee, "The Place of Privacy in Data Protection Law" (2001) 24(1) *University of New South Wales Law Journal* 6

Carney, Terry, "Where Now Australia's Welfare State" (2013) *iv Diritto Pubblico Comparato ed Eurpeo [Journal of Comparative and European Public Law]* 1353

Charlesworth, Hiliary, Madelaine Chaim, Devika Hovell and George Williams, "Deep Anxieties: Australia and the International Legal Order" (2003) 25 *Sydney Law Review* 423

Carney, Terry, "Neoliberal Welfare Reforms and "Rights" Compliance Under Australian Social Security Law" (2006) 12(1) *Australian Journal of Human Rights* 223

Carter, Meredith, "Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers" (2002) 172 *Medical Journal of Australia* 28

Chambers, Simone, "Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation" (2004) 12 *Journal of Political Philosophy* 389

Coiera, Enrico and Johanna Westbrook, "Should Clinical Software Be Regulated?" (2006) 184 (12) *Medical Journal of Australia* 600

Connolly, Chris, "Managing Patient Consent in a Multidisciplinary Team Environment – KJ v Wentworth Area Health Services and its Implications for HRIPA" (2004) 11(2) *Privacy Law and Policy Reporter* 29

Cornwell, Amanda, "NSW Electronic Health Records Get Serious" (2000) 7 *Privacy Law and Policy Reporter* 80

Editorial Comment, "The Right to Privacy in Nineteenth Century America" (1981) *Harvard Law Review* 1892

Edelmann, Lauren, Sally Fuller and Iona Mara-Drita, "Diversity Rhetoric and the Managerialization of Law" (May 2001) 106(6) *American Journal of Sociology* 1589

Fichman, Robert, Rajiv, Kohli and Ranjani Krishnan, "The Role of Information Systems in Healthcare: Current Research and Future Trends" (September 2011) 22(3) *Information System Research* 419

Foster, Bryan and Yvette Lejins, 'E-Health Security in Australia: The Solution Lies with Frameworks and Standards' (Paper Presented to Australian eHealth Informatics and Security Conference, July 2013)

Fried, Charles, "Privacy" (1968) 77 *Yale Law Journal* 475

Gay, Rebekah, "Mainstreaming Wellbeing: An Impact Assessment for the Right to Health" (2008) 13(2) *Australian Journal of Human Rights* 33

Gavison, Ruth, "Too Early for a Requiem: Warren and Brandeis were Right on Privacy v Free-Speech" (1992) 43 *South Carolina Law Review* 437

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

Gellman, Robert, "The Marketing Exceptions in U.S. Health Privacy Rules" (2001) 7(8) *Privacy Law and Policy Reporter* 164

Gerber Paul, "Confidentiality and the Courts" (1999) 170 *Medical Journal of Australia* 22

Gerber, Paul, "Late-term Abortion: What Can Be Learned from Royal Women's Hospital v Medical Practitioners Board of Victoria?" (2 April 2007) 186 (7) *Medical Journal of Australia* 359

Gerety, Tom, "Redefining Privacy" (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 233

Godkin, E R, "The Rights of the Citizen – To His Own Reputation" (July-December 1890) *Scribner's Magazine* 65

GodKin, E R, "Libel and its Legal Remedies" (1880) 12 *Journal of Social Science* 69

Graven, Baxton, "Personhood: The Right to be Let Alone' (1976) 6 *Duke Law Journal* 699

Greenleaf, Graham, "Australia's Proposed ID Card: Still Quacking like a Duck" [2007] *University of New South Wales Faculty of Law Research Series* 1; (2007) 23 *Computer Law and Security Report*

Greenleaf, Graham, "Access All Areas: Function Creep Guaranteed in Australia's ID Card Bill (No.1)" [2007] *University of New South Wales Faculty of Law Research Series* 11; (2007) 23 *Computer Law and Security Report*

Greenleaf, Graham, "Function Creep - Defined and Still Dangerous in Australia's Revised ID Card Bill" [2007] *University of New South Wales Faculty of Law Research Series* 64; (2008) 24(1) *Computer Law and Security Report* 56

Greenleaf, Graham, "An Endnote on Regulating Cyberspace: Architecture vs Law?" (1998) 21(2) *University of New South Wales Law Journal* 593

Greenleaf, Graham, Nigel Waters and Lee Bygrave, "Implementing Privacy Principles: After 20 Years, It's Time to Enforce the Privacy Act" [2007] *University of New South Wales Faculty of Law Research Series* 31; Submitted to the ALRC on the Review of Privacy Issues Paper (January 2007)

Gross, Hyman, "The Concept of Privacy" (1967) 43 *New York University Law Review* 34

Hart, Caroline, "Micro-Chipping Away at Privacy: Privacy Implications Created by the New Queensland Driver Licence Proposal" [2007] 7(2) *Queensland University of Technology Law and Justice Journal* 19

Holman, D'Arcy, J, A John Bass, Diana L Rosman and Merran B Smith, James B Semmens, Emma J Glasson and Emma L Brook, Brooke Trutwein, Ian L Rouse, Charles R Watson, Nicholas H de Klerk and Fiona J Stanley "A Decade of Data Linkage in Western Australia: Strategic Design, Applications and Benefits of the WA Data Linkage System" (November 2008) 32 *Australian Health Review* 4

Horrigan, Bryan, "Reforming Rights-Based Scrutiny and Interpretation Legislation" (2012) 37(4) *Alternative Law Journal* 228

Ihde, Don, "Technoscience and 'Other' Continental Sciences" (2005) 3 *Philosophical Problems Today* 91

Ihde, Don, "Technoscience and the 'Other' Continental Philosophy" (2000) 33(1) *Continental Philosophy Review* 59

Jones, R V H and S Jane Richards, "Confidentiality and Medical Records" (March 1978) *Journal of the Royal College of General Practitioners* 137

Jourard, Sidney, "Some Psychological Aspects of Privacy" (1966) 31 *Law and Contemporary Problems* 307

Kalven, Harry, "Privacy in Tort Law: Were Warren and Brandeis Wrong?" (1966) 31 *Law and Contemporary Problems* 326

Klein, Carolina, (2011) "Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care" 39 *Journal American Academy of Psychiatry Law* 571

Kosseim, Patricia and Megan Brady, "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes "[2008] 2 *McGill Journal of Law and Health/Revue De Droit Et Sante De McGill* 12

Killey, I, "Peace, Order and Good Government: A Limitation on Legislative Competence" (1989) 17 *Melbourne University Law Review* 25

Kramer, Irwin, "The Birth of Privacy Law: A Century Since Warren and Brandeis" (1990) 39 *Catholic University Law Review* 703

Lacovino, Livia, "Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect*" (2004) 12 *Journal of Law and Medicine* 40

Lindberg, Donald and Betsy Humphreys, "Medicine and Health on the Internet" (1998) 280 *Medical Journal of Australia* 1303

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

Lium, Jan Tore and Arild Faxvaag, "Removal of Paper-Based Health Records From Norwegian Hospitals: Effects on Clinical Workflow" (2006) 124 *Studies in Health Technology and Informatics* 1031-1036

Livia, Lacovino, "Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect*" (2004) 12 *Journal of Law and Medicine* 40

Lloyd, Halani, "Are Privacy Laws More Concerned with Legitimising the Data Processing Practices of Organisations than Safeguarding the Privacy of Individuals?" (2002) 9(5) *Privacy Law and Policy Reporter* 81

Ludwick, D A and John Doucette, "Adapting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries" (2009) 78 *International Journal of Medical Informatics* 22

MacRae, Damien, "Telehealth and the Law: If Uncertainty Persists, Please Consult Your Lawyer" (1999) 6 *Journal of Law and Medicine* 270

Mariotti, Humberto, 'Autopoiesis, Culture, and Society (online) http://www.oikos.org/mariotti.htm (viewed on 15/9/2014)

McCormick, D, "Privacy: A Problem of Definition" (1974) 1 *British Journal of Law and Society* 75

Magnusson, Roger, "Confidentiality and Consent in Medical Research: Some Recurrent, Unresolved Legal Issues Faced by IECs" (1995) 17 *Sydney Law Review* 549

Magnusson, Roger, "Data Linkage: Health Research and Privacy: Regulating Data Flows in Australia's Health Information System" (2002) 24 *Sydney Law Review* 5

Magnusson, Roger, "The Changing Legal and Conceptual Shape of Health Care Privacy" (2004) 32(4) *Journal of Law, Medicine and Ethics* 680

Mainsbridge, Anne, "Employers and Genetic Information: A New Frontier for Discrimination" (2002) 2 *Macquarie Law Journal* 61

Manin, Bernard, "On Legitimacy and Political Deliberation" (1987) 15 *Political Theory* 338

McBeth, Adam, "Privatising Human Rights: What Happens to the State's Human Rights Duties When Services are Privatised?" (2004) 5(1) *Melbourne Journal of International Law* 133

McSherry, Bernadette, "Ethical Issues in Health*Connect's* Shared Electronic Health Records System" (2004) 12 *Journal of Law and Medicine* 60

McSherry, Bernadette, "Third Party Access to Shared Electronic Mental Health Records: Ethical Issues (2004) 11(1) *Psychiatry, Psychology and Law*

McSherry, Bernadette, "Health Professional Patient Confidentiality: Does the Law Really Matter?" (2009) 15(4) *Journal of Law and Medicine* 489

McRae, L, "Withholding Medical Records Without Explanation: A Foucauldian Reading of Public Interest" (2009) 17(3) *Medical Law Review* 438

Mendelson, Danuta, "Mr Cruel and the Medical Duty of Confidentiality" (1993) 1(2) *Journal of Law and Medicine* 120

Mendelson, Danuta, "Medical Confidentiality in Australian and Jewish Law" (1997) 12 *The Jewish Law Annual* (The Institute of Jewish Law, Boston University School of Law) 217

Mendelson, Danuta, "Medical Duty of Confidentiality in the Hippocratic Tradition and Jewish Medical Ethics" (1998) 5(3) *Journal of Law and Medicine* 227

Mendelson, Danuta, "Judicial Responses to the Protected Confidentiality Communications Legislation in Australia" (2002) 10 *Journal of Law and Medicine* 49

Mendelson, Danuta, "Travels of a Medical Record and the Myth of Privacy" (2003) 11(2) *Journal of Law and Medicine* 136

Mendelson, Danuta, "Devaluation of a Constitutional Guarantee: The History of Section 51 (XXIIIA) of the Commonwealth Constitution" (2003) 23 *Melbourne University Law Review* 308

Mendelson, Danuta, "Electronic Medical Records: Perils of Outsourcing and the *Privacy Act 1988* (Cth)" (2004) 12(1) *Journal of Law and Medicine* 8

Mendelson, Danuta, "Health*Connect* and the Duty of Care: A Dilemma for Medical Practitioners" (2004) 12 *Journal of Law and Medicine* 69

Mendelson, Danuta, "Healthcare Identifiers Legislation: A Whiff of Fourberie" (2010) 17 *Journal of Law and Medicine* 660

Mendelson, Danuta, "The Duchess of Kingston's Case, The Ruling of Lord Mansfield and Duty of Medical Confidentiality in Court" (2012) 35(5-6) *International Journal of Law and Psychiatry* 480

Mirzaian, Aristotle, "Y2K Who Cares? We Have Bigger Problems: Choice of Law in Electronic Contracts" (2000) 6 *University of Richmond Journal of Law and Technology* 4

Mulligan, Ea, "Confidentiality in Health Records: Evidence of Current Performance from a Population Survey in South Australia" (2001) 174 *Medical Journal of Australia* 637

Murphy, Richard, "Property Rights in Personal Information: An Economic Defense of Privacy" (1996) 84 *Georgetown Law Journal* 2381

Mould, Annie, "Implications of Genetic Testing: Discrimination in Life Insurance and Future Directions" (2003) 10(4) *Journal of Law and Medicine* 1

Morozov, Evengy, "The Real Privacy Problem" (22 October 2013) 116 (6) *MIT Technology Review* 32

Morozov, Evengy, "Iran: Downside to the 'Twitter Revolution'" (1 October 2009) 56(4) *Dissent* (00123846) 10

Mount, Christopher, Christopher Kelman, Leonard Smith and Robert Douglas "An Integrated Electronic Health Record and Information System for Australia" (2000) 172 *Medical Journal of Australia* 25

Myers, Julie, Thomas Frieden, Kamal Bherwani and Kelly Henning, "Ethics in Public Health Research: Privacy and Public Health Risk: Public Health Confidentiality in the Digital Age" (May 2008) 98(5) *American Journal of Public Health* 793

Nicholas, Terry, "Electronic Health Records: International, Structural and Legal Perspectives (2011) 12 *Journal of Law and Medicine* 26

Nicholas, Terry and Leslie Francis, "Ensuring the Privacy of Confidentiality of Electronic Health Records" (2007) 2 *University of Illinois Law Review Journal* 681

O'Keefe, Christine and Chris Connolly "Privacy and the Use of Health Data for Research" (2010) 193(9) *Medical Journal of Australia* 537

Ohlden, Ann, 'Landmark Resolution Passed to Preserve the Future of Privacy, Adoption of Design as an International Standard' (Paper Presented at International Data Protection and Privacy Commissioners, Jerusalem, 29 October 2010)

Otlowski, Margaret, "Protecting Genetic Privacy in the Research Context: Where to From Here?" (2002) 2 *Macquarie Law Journal* 4

Otlowski, Margaret and Robert Williamson, "Ethical and Legal Issues and the 'New Genetics'" (2003) 178 *Medical Journal of Australia* 582

Parent, W A, "Recent Work on the Concept of Privacy" (1993) 20 *American Philosophical Quarterly* 341

Parent, W.A, "A New Definition for Privacy for the Law" (1983) 2 *Law and Philosophy* 305

Paterson, Moira, "Health*Connect* and Privacy: A Policy Conundrum" (2004) 12 *Journal of Law and Medicine* 8

Parker, Richard, "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275

Paterson, John, "Australian Health Care Agreements 2003-2008: A New Dawn?" (2002) 6 *Medical Journal of Australia* 177

Pearce, Christopher and Mukush Haikerwal, "E-health in Australia: Time to Plunge into the 21st Century" (2010) 193(7) *Medical Journal of Australia* 397

Prosser, William, "Privacy: A Legal Analysis" (1960) 48 *California Law Review* 338

Reiman, J, "Driving to the Panopticon" (1995) 11 *Santa Clara Computer and High Technology Law Journal* 27

Richardson, Megan, "Whither Breach of Confidence: A Right of Privacy for Australia?" (2002) 26 *Melbourne University Law Review* 381

Rosen, Jeffrey, "The Naked Crowd: Balancing Privacy and Security in an Age of Terror" (2004) 46 *Arizona Law Review* 607

Rosen, Jeffrey, 'The Naked Crowd: Balancing Privacy and Security in the Age of Terror' (Paper presented at Twenty-Fourth Annual Isaac Marks Memorial Lecture on 4 March 2004, Philadelphia)

Rosenbaum, Joseph, "Privacy on the Internet: Whose Information Is It Anyway?" (1998) 38 *Jurimetrics Journal* 565

Rubenfeld, Jed, "The Right to Privacy" (1989) 102 *Harvard Law Review* 737

Scanlon, Thomas, "Thomas on Privacy" (1966) 4 *Philosophy and Public Affairs* 315

Sherer, Andeas Georg and Guido Palazzo, "The New Political Role of Business in a Globalised World: A New Perspective on CSR and its Implications for Firm, Governance and Democracy" (4 June 2011) 4 *Journal of Management Studies* 48

Shils Edward, "Privacy its Constitution and Vicissitudes" (1966) 31 *Law and Contemporary Problems* 281

Shillemans, T, "Accountability in the Shadow of Hierarchy: The Horizontal Accountability of Agencies" (2008) 8 *Public Organisation Review* 175

Schwartz, Paul, "Privacy and Democracy in Cyberspace" (1999) 52 *Vanderbilt Law Review* 1609

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

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

Samuels, A, "Privacy: Statutorily Definable?" (1996) 17 *Statute Law Review* 115

Savulescu, Julian, Iain Chalmers and Jennifer Blunt, "Are Research Committees Behaving Unethically? Some Suggestions for Improving Performance and Accountability" (1996) 313 (7069) *British Medical Journal* 1390

Simitis, Spiro, "From Market to the Polis: The EU Directive on the Protection of Personal Data" (1994) 80 *Iowa Law Review* 445

Simitis, Spiro, "Reviewing Privacy in an Information Society" (1987) 135(3) *University of Pennsylvania Law Review*

Simitis, Spiro, 'Privacy Lecture' (Paper Presented at Berkeley University Law School, Berkeley California USA, April 2010)

Stanton, Jeffrey and Kathryn Stam, "Information Technology, Privacy, and Power within Organisations: A View from Boundary Theory and Social Exchange Perspectives" (2003) 1(2) *Journal of Surveillance & Society* 152

Stern, Jon and Stuart Holder, "Regulatory Governance: Criteria for Assessing the Performance of Regulatory Systems: An Application to Infrastructure Industries in the Developing Countries of Asia" (1999) 8 *Utilities Policy* 33

Stone, Alan, "The Tarasoff Decision: Suing Psychotherapists to Safeguard Society" (December 1976) 90(2) *Harvard Law Review* 358

Svantesson, Dan Jerker, "Privacy, the Internet and Transborder Data Flows: An Australian Perspective" (2007) 19 *Bond Law Review* 1

Taylor, Greg, "Federalism in Australia" [2010] *Melbourne University Law Research Series* 11; (2011) 4 *International Constitutional Law* 171

Tene, Omer and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics (April 2013) 11 (5) *Northwestern Journal of Technology and Intellectual Property* 239

Teubner, G, "Self-Constitutionalizing TNCs? On the Linkage of 'Private' and 'Public' Corporate Codes of Conduct" (2011) 18 *Indiana Journal of Global Legal Studies* 617

Thiede, Michael, "Information and Access to Halth Care: Is There a Role for Trust?" (2005) *Journal of Social Science and Medicine* doi:10.1016/j.socsimed.2004.11.076 (online)

Toohey, Justice John, "A Government of Laws, and Not of Men?" (1993) 4 *Public Law Review* 158

Turkington, Richard, "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Privacy" (1990) 10 *Northern Illinois University Law Review* 479

Walker, Geoffrey, "Dicy's Dubious Dogma of Parliamentary Sovereignty" (1985) 59 *Australian Law Journal* 276

Warden, James, "Federalism and the Design of the Australian Constitution" (1992) 27 *Australian Journal of Political Science* 143

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

Weeks, Greg, 'The Use and Enforcement of Soft Law by Australian Public Authorities' (Paper Presented at the Practice and Theory of Soft Law Academic Symposium, Peking University, 9 July 2011); (2014) 42(1) *Federal Law Review* 181

Westin, Alan, "Privacy and Freedom" (1968) 25 *Washington & Lee Law Review* 1

Westin, Alan, "Social and Political Dimensions of Privacy" (29 April 2003) 59(2) *Journal of Social Issues* 431

Wheelwright, K, "Commonwealth and State Powers in Health – A Constitutional Diagnosis" (1995) 21(1) *Melbourne University Law Review* 53

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

Zarsky, Tal, "Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion" (2003) 5(1) *Yale Journal of Law and Technology* 1

D GOVERNMENT DOCUMENTS/DEBATES

Auditor-General for Australia, Pat Barrett, 'Public Private Partnerships – Are There Gaps in Public Sector Accountability?' (Paper Presented at 2002 Australasian Council of Public Accounts Committee Seventh Biennial Conference, Melbourne Australia, 3 February 2003)

Australia-US Free Trade Agreement (AUSFTA) signed in 2004

Australian Bureau of Statistics, '8153.0 – Internet Activity, Australia June 2010'

Australian Bureau of Statistics, '8153.0 – Patterns of Home Internet Use 2014

Australian Bureau of Statistics, '8153.0 – Personal Internet Use 2012

Australian Bureau of Statistics, 8153.0 – Australian Population Clock 2015

Australian Bureau of Statistics, 8153.0 –Australian Historical Statistics 2014

Australian Capital Territory Health Services, *Your Rights and Responsibilities* (2006)

Australian Government, *A National Information Health and Network for Australia* (June 2010)

Australian Government, Financial and Analysis Branch Commonwealth Department of Health and Aged Care, *The Australian Health Care System: An Outline* (September 2000)

Australian Government, Healthbase Australia, *Australia, Personally Controlled Electronic Health Records, Change and Adoption Partners - $29.9 Million* (2012)

Australian Government, National E-Health Transition Authority (NEHTA), *Draft Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System* (July 2011)

Australian Government, National E-Health Transition Authority (NEHTA), *Concepts of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Records System* (September 2011)

Australian Government, *Enhancing National Privacy Protection Australian Government First Stage Response to the ALRC: Report 108* (October 2009)

Australian Government, Department of Finance and Deregulation, *Cloud Computing Strategic Directions Paper – Draft Consultation* (January 2011)

Australian Government, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (September 2011)

Australian Government, *National Health Reform: Progress and Delivery* (September 2011)

Australian Government, Council of Australian Government (COAG), *Healthcare Identifiers and Privacy: Discussion Paper on Proposal for Legislative Support* (July 2009)

Australian Government, Council of Australian Government (COAG), *Personally Controlled Electronic Health Records System: Legislation Issues Paper* (April 2011)

Australian Government, *First Stage Response to the Australian Law Reform Commission Recommendations* (2009)

Australian Government, Department of Finance and Deregulation, Government 2.0 Taskforce, *Engage – Getting on with Government 2.0* (December 2009)

Australian Government, National Health Reform Committee, *A National Health and Hospitals Network for Australia's Future Delivering the Reforms* (2010)

Australian Government, *Review of the Law of Negligence, Final Report* ('Ipp Report') (October 2002)

Australian Health Information Council (AHIC), *E-Health Future Directions Briefing Paper for AHMAC Meeting* (4 October 2007)

Australian Institute of Health and Welfare (AIHW), *Australia's Health 2010* (May 2010)

Australian Health Ministers' Advisory Council, *A Streamlined National Approach to Scientific and Ethics Review of Multi-Centre Health and Medical Research in Australia* (September 2006).

Australian Health Minister's Council (AHMC), *Joint Communique* (13 July 2009)

Australian Health Practitioner Regulation Agency (AHPRA), *Delegations Under the National Law*, LPN 22, 3 February 2014

Australian Health Practitioner Regulation Agency (AHPRA), *Court or Tribunal Power to Stay a Board Decision*, LPN 21, 18 October 2013

Australian Institute of Health and Welfare (AIHW), *Australia's Health 2010* (May 2010)

Australian Law Reform Commission (ALRC), *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws*: Issues Paper 46 (December 2014)

Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era – Final Report*: Report 123 (3 September 2014)

Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era:* ALRC 123 Summary) (3 September 2014)

Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era:* Discussion Paper 80 (March 2014)

Australian Law Reform Commission (ALRC), *Copyright and the Digital Economy:* Summary Report 122 (November 2013)

Australian Law Reform Commission (ALRC), *Serious Invasions of Privacy in the Digital Era:* Issues Paper 43 (October 2013)

Australian Law Reform Commission (ALRC), 'Research: Databases and Data Linkage' in *Report 108 - For Your Information: Australian Privacy Law and Practice* (October 2009) 66

Australian Law Reform Commission (ALRC), *Review of Australian Privacy:* Discussion Paper 72 (September 2008)

Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Laws and Practice:* Report 108 (12 August 2008)

Australian Law Reform Commission (ALRC), Executive Summary, *Extensive Public Engagement:* Report 108 (11 August 2008)

Australian Law Reform Commission (ALRC), *Review of Australian Privacy Law:* Discussion Paper 72 (12 September 2007)

Australian Law Reform Commission, *Invasion of Privacy: Consultation Paper 1* (2007)

Australian Law Reform Commission (ALRC), *Review of Privacy:* Issues Paper 31 (9 October 2006)

Australian Law Reform Commission (ALRC), *For Your Information: Australia's Privacy Law and Practice:* Report No 32 (2006)

Australian Law Reform Commission (ALRC) and Australian Health Ethics Committee (AHEC), *Essentially Yours: The Protection of Human Genetic Information in Australia* (30 May 2003)

Australian Law Reform Commission (ALRC) and Australian Health Ethics Committee, *Protection of Human Genetic Information:* Discussion Paper 66 (August 2002)

Australian Law Reform Commission (ALRC), *Australia's Federal Records: A Review of Archives Act 1983*: Final Report 85 (30 July 1998)

Australian Law Reform Commission (ALRC), *Privacy*: Report 22 (15 December 1983)

Australian Law Reform Commission (ALRC), *Unfair Publication: Defamation and Privacy*: Report 11 (7 June 1979)

Australian Medical Association (AMA), 'Personal Control Versus Clinical Need for Complete Unedited Records' (Press Release 26 November 2013)

Australian Medical Association (AMA), *Code of Ethics* (2006), 1.1 (12) under 'Patient Care' 1.1 (13)

Australian Medical Association's (AMA) *Code of Ethics* (2003). 1.1.1. http://www.ama.com.au/codeofethics (viewed on 12/6/2012).

Australian Medical Association (AMA), to Department of Health and Aged Care, on *Submission to the Commonwealth Department of Health and Aged Care: The Better Medication Management System: Draft Exposure Legislation,* July 2001

Australian Privacy Foundation, to Australian Health Minister's Advisory Council, *Australian Privacy Foundation Responses to Australian Health Minister's Advisory Council Paper,* July 2009

Australian Privacy Foundation, to Australian Health Minister's Advisory Council, on *Submission to Exposure Draft, Healthcare Identifiers Bill,* August 2009

Boston Consulting Group (BCG), *National Health Information Management and Information and Communications Technology Strategy* (August 2004)

Boston Consulting Group (BCG), *Report on the NEHTA Review* (October 2007)

Clayton Utz, to Office of the Australian Privacy Commissioner, *National E-Health Transition Authority Unique Healthcare Identifier Program Privacy Impact Statement* (3 March 2008)

Choo, Raymond Kwang, Australian Institute of Criminology, *Cloud Computing: Challenges and Future Directions* (October 2010)

Commonwealth Government, *Health Online: A Health Information Action Plan for Australia* (November 1999)

Commonwealth Government, *Health Online* (2nd ed, September 2001)

Commonwealth Parliament, House of Representatives, *Parliamentary Debates* (No 15749, Parliamentary Debates, 12 April 2000) (D Williams Attorney-General)

Council of Australian Government (COAG), *Joint Communique: New Council a Vital Link to Future Health Information Management Australia* (28 November 2003)

Council of Australian Government (COAG), *Australian Health Ministers Cooperation Towards National Health Care* (April 2001)

Council of Australian Government (COAG), *National Health Agreement 2011* (2011)

Council of Australian Government (COAG), *National Health Agreement 2012-2013* (2012)

Consumer Health Forum (CHF), to Australian Government, on *Consumer Health Forum Response to the Concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System*, October 2011

Commonwealth Government, *Government Response to the Senate Legal and Constitutional Reference Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006)

Consumer Health Forum (CHF), to Senate Legal and Constitutional Reference Committee, on *Consumer Health Forum Response to the Concept of Operations Relating to the Introduction of a Personally Controlled Electronic Health Record System,* October 2011

Consumer Health Forum (CHF), to Senate Legal and Constitutional Reference Committee, on *CHF Submission on the Healthcare Identifiers and Privacy: Discussion Paper on Proposal for Legislative Support,* August 2009

Council of Australian Governments (COAG), to Senate Legal and Constitutional reference Committee, *Healthcare Identifiers and Privacy: Discussion Paper on Proposals for Legislative Support* (July 2009)

Council of Australian Governments (COAG), *National Health Care Agreement 2003-2008* (2003)

Council of Australian Governments (COAG), *National Health Agreement 2011* (2011)

Council of Australian Governments (COAG), *National Partnership Agreement on E-Health Schedule A* (2009)

CSC Pty Ltd, '*Healthcare Research Report: A Rising Tide of Expectations: Australian Consumers' Views on Electronic Health Records – A Necessary Ingredient to Healthcare Reform* (Report July 2010)

Deloitte, to Department of Health and Ageing (Cth), *Department of Health and Ageing National E-Health Conference Report* (Report March 2011)

Deloitte, National E-Health and Information Principle Committee, *National E-Health Strategy* (30 September 2008)

Department of Broadband, Communication and the Digital Economy (Cth), *National Broadband Network – Overview* (2013)

Department of Broadband, Communications and the Digital Economy (Cth), *National Digital Economy Strategy* (2009)

Department of Communication, Information, Technology and the Arts (Cth), *Information Economy: Identifying Priorities of Action* (1998)

Department of Communication, Information Technology and the Arts (Cth), *A Strategic Framework for the Information Economy: Identifying Priorities for Action* (December 1998)

Department of Education, Science and Training (Cth), *National Collaborative Research Infrastructure Strategy* (2004)

Department of Finance and Deregulation (Cth), *Cloud Computing Strategic Direction Paper – Draft Consultation* (January 2011)

Department of Health and Ageing (Cth), to Office of Australian Privacy Commission on *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988* (December 2004)

Department of Health and Ageing (Cth), *MediConnect: Linking Medicines Information: Report* (January 2005)

Department of Health and Ageing (Cth), *Department of Health and Ageing National E-Health Conference Report* (March 2011)

Department of Health and Ageing (Cth), *Personally Controlled Electronic Health Record System: Legislation Issues Paper* (September 2011)

Department of Prime Minister and Cabinet of Australia (DPMC), *Commonwealth-State Ministerial Councils: A Compendium* (1994)

Department of the Prime Minister and Cabinet, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (September 2011)

Dreyfus, M, House of Representatives, 'Second Reading Speech: Privacy Amendment (Privacy Alerts) Bill 2013 Debate' *Alerts Digest*, 2013

Galexia, *Preliminary PIA Healthcare Identifiers and Individual Healthcare Provider Final Report v19* (7 May 2006)

Government of South Australia, Department of Health South Australia, *Your Rights and Responsibilities: A Charter for South Australian Public Health Consumers* (2005)

Greenleaf, Graham, to the Senate Legal and Constitutional Affairs Committee, on *Submission 59* (2009)

Federal Liberal Coalition Government, *The Coalition's Policy to Support Australia's Health System* (August 2013)

Federal Liberal Coalition Government, *The Coalition's Policy for E-Government and the Digital Economy* (September 2013)

Federal Liberal Coalition Government of Australia, Federal *Budget* 2014-2015

Federal Liberal Coalition Government of Australia, Federal *Health Budget* 2014

Federal Labor Government of Australia, Federal *Budget* 2010-2012

Healthbase Australia, Personally Controlled Electronic Health Records (Cth), *Change and Adoption Partner - $29.9 million* (2012) http://www.healthbase.info/pcehr/page19/page20/page20.html (viewed on 30/3/2013)

Health*Connect* Program Office (Cth), *Consent and Electronic Records: A Discussion Paper* (July 2002)Health*Connect* (Cth), *HealthConnect and the Information Management and Information Communications Technology Industry* (2003)

Health*Connect* (Cth), *What is HealthConnect?* (November 2003)

Health*Connect* (Cth), *HealthConnect Interim Report: Overview and Finding* (August 2003)

Health*Connect* (Cth), *Northern territory Interim Report* (February 2003)

Health*Connect* (Cth), *North Queensland Trial Qualitative Feedback* (November 2004)

Health*Connect* (Cth), *Tasmanian HealthConnect Trial Phase 1 Final Report* (November 2004)

Health*Connect* (Cth), *Evaluation of the Field Test of MediConnect* (January 2005)

Health*Connect* (Cth), *Lessons Learnt in the MediConnect Field Test and HealthConnect Trials* (April 2005)

Health*Connect* (Cth), *New South Wales and Queensland HealthConnect and MediConnect Trials 2004-2005* (2005)

Health*Connect* (Cth) and Dr Brian Richards, National Director E-Health Implementation Australia, *E-Health Implementation Stakeholders Perspective* (25 November 2005)

Jolly, Rhonda, Department of Parliamentary Services, *Healthcare Identifiers Bill 2010*, Law and Bills Digest No 116 of 2010, 24 February 2010

Jolly, Rhonda, 'The E-Health Revolution – Easier Said Than Done' (Research Paper No 3, Parliamentary Library, Parliament of Australia, 17 November 2011)

Jolly, Rhonda, Department of Parliamentary Services, *Personally Controlled Electronic Health Records Bill 2011*, Law and Bills Digest No 100 of 2011-2012, 7 February 2012

Law Council of Australia (LCA), to Attorney-General of Australia, on *Submission to the Attorney-General's Department Discussion Paper on Australian Privacy Breach Notification,* 29 November 2012

Law Council of Australia, to Senate Legal and Constitutional Affairs Committee, on *Submission to Senate Legal and Constitutional Affairs Committee Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012,* July 2012

Law Council of Australia, to Attorney-General's Department, on *Submission to Attorney-General's Department Discussion Paper on Australian Privacy Breach Notification*, 29 November 2012

Lim, Kean-Seng, National Electronic Health Transition Authority (NEHTA) Clinical Lead, *The Personally Controlled Electronic Health Record (PCEHR) and the General Practitioner* (3 April 2013)

Ludwig, Joe, Cabinet Secretary, *Companion Guide to Australian Privacy Principles* (Department of Parliamentary Services No 6, Parliament of Australia, 2006)

Mallesons Stephen Jaques, to Office of Australian Privacy Commissioner, *Privacy Impact Assessment Individual Healthcare Identifiers* (Report July 2009)

Martin, L, *Awareness, Trust and Security to Shape Government Cloud Adoption: A White Paper* (April 2010)

McMillan, J, Department of the Senate, *Constitutional Reform in Australia,* Parliamentary Paper No 13, November 1991

Medical Board of Australian, *Good Medical Practice Code*, 3.4 (current)

Medi*Connect*, *MediConnect Field Test Evaluation – Launceston Phase 1* (October 2003)

Medi*Connect*, *Evaluation of the Field Test of MediConnect: Fourth Evaluation Field Visits to Launceston and Ballarat* (November 2004)

Mitchell, John, National Office for the Information Economy, Department of Communication, *From Telehealth to E-Health: The Unstoppable Rise of E-Health* (1999)

National Electronic Health Records Taskforce, *A National Approach to Electronic Health Records for Australia* (March 2000)

National Electronic Health Records Taskforce, *A Health Information Network for Australia* (July 2000)

National Health Information Standards Advisory Committee (NHISAC), *Setting the Standards: A National Health Information Standards Plan for Australia* (February 2001)

National E-Health Transition Authority (NEHTA), *Privacy Blueprint for the Individual Electronic Record* (February 2006)

National E-Health Transition Authority (NEHTA), *NEHTA's Approach to Privacy* (4 July 2006)

National E-Health Transition Authority (NEHTA), *Privacy Blueprint – Unique Identifiers* Version 1.0 (18 December 2006)

National E-Health Transition Authority (NEHTA), *Frontiers in Healthcare Delivery* (2007)

National E-Health Transition Authority (NEHTA), *The Right Healthcare, The Right Future, The Right Answer* (2008)

National E-Health Transition Authority (NEHTA), *Shaping the Future of Healthcare: Privacy Blueprint for the Individual Electronic Health Record* (2008)

National E-Health Transition Authority (NEHTA), *Privacy Blueprint for the Individual Electronic Health Record* (3 July 2008)

National E-Health Transition Authority (NEHTA), E-*Health Record: Shaping the Future of Healthcare* (September 2008)

National E-Health Transition Authority (NEHTA), *A Healthier Future for all Australians: Final Report* (June 2009)

National E-Health Transition Authority (NEHTA) (Cth), *E-Health Healthcare Today* (July 2010)

National E-Health Transition Authority (NEHTA), *Blueprint on Privacy* Version 1.0, Draft for Consultation (13 August 2010)

National E-Health Transition Authority (NEHTA) (Cth), *E-Health Information Security: National E-Health Security and Access Framework* (NESAF) (2010)

National E-Health Transition Authority (NEHTA) (Cth), *Healthcare Identifiers Service Implementation Approach* (2010)

National E-Health Transition Authority, *Draft Concepts of Operations for Personally Controlled Electronic Health Records (PCEHR)* (April 2011)

National E-Health Transition Authority (NEHTA), *E-Health Strategic Plan Refresh 2011/2012* (2011)

National e-Health Transition Authority (NEHTA), *Concept of Operations: Relating the Introduction of a Personally Controlled Electronic Health Record System (PCEHR)* (September 2011)

National E-Health Transition Authority (NEHTA), *Latest News-Software Developers to Engage with National E-Health Records System Ahead of July 2012 Launch* (July 2012)

National E-Health Transition Authority (NEHTA), *PCEHR Lead Sites* (2012)

National E-Health Transition Authority (NEHTA), *Standards Australia Specification ATS 5820 for E-Health Web Services Profiles* (2013)

National E-Health Transition Authority (NEHTA), *Next Step After You Receive Identity Verification Code* (2013) <http://e-health.gov.au/internet/ehealth/publishing.nsf/Content/brochure-ivc (viewed on 23/7/2013)

National E-Health Transition Authority (NEHTA), *E-Health Architecture, Interoperability and Standards* http://www.neta.gov.au/connecting-australia/e-health-architecture (viewed on 15/4/13)

National E-Health Transition Authority (NEHTA), *Standards Australia Technical Specification ATS 5821 for E-Health XML Secured Payload Profiles* (2013)

National E-Health Transition Authority (NEHTA), *The Best and Worst of Cloud Contracts* (8 March 2013)

National E-Health Transition Authority (NEHTA), *E-Health Fact Sheet – Prescribed and Dispensed Medication* (2013)

National Health Information Management Advisory Council, *Health Online, A Health Information Action Plan for Australia* (2nd ed, September 2001)

National Health Information's Standards Advisory Committee, *Setting the Standards: A National Health Information Standards Plan for Australia* (February 2001)

National Health Information Management Advisory Council, *A Health Information Action Plan for Australia* (2nd ed, 2001)

National Health Information Management Advisory Council Review Steering Group, *Review of the National Health Information Management Advisory Council: Issues Paper* (2002)

National Health and Medical Research Council (NHMRC), *Guidelines Approved under Section 95A of the Privacy Act 1988 (Cth)* (December 2001)

National Health and Medical Research Council (NHMRC), *Monitoring Activities of the HRECs' Sets out HREC Annual Report Requirement* (2003)

National Health and Medical Research Council (NHMRC), *National Research Priority and National Health Priority* (2003-2006) (2003)

National Health and Medical Research Council (NHMRC), Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle for a Healthy Competitive Australia* (2004)

National Health and Medical Research Council (NHMRC), *National Statement on Ethical Conduct in Human Research* (2007)

National Health and Medical Research Council (NHMRC), *NHMRC Strategic Plan 2003-2006* (2006)

National Health and Medical Research Council (NHMRC), *Working to Build a Healthy Australia* (2006)

National Health and Medical Research Council (NHMRC), *National Statement on Ethical Conduct in Human Research* (2007)

National Electronic Health Records Taskforce, *A Health Information Network for Australia: Report to Health Minister by the National Electronic Health Records Taskforce* (July 2001)

Neilsen Mary Anne and Jonathan Chown, Department of Parliamentary Services, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Law and Bill Digest No 20 of 2012-2013, 7 November 2012

Neilson, Mary Anne, Department of Parliamentary Services, *Privacy Amendment (Privacy Alerts) Bill 2013*, Law and Bills Digest No 146, 2012-2013, 19 June 2013

New South Wales Health, *Privacy Internal Review Guidelines NSW Health* (2006)

New South Wales, Legislative Assembly, *Parliamentary Debates* No 18872-18874, 28 October 2009 (Carmel Tebbutt, Minister of Health)

New South Wales Law Reform Commission (NSWLRC), *Consultation Paper 1: Invasion of Privacy* (May 2007)

New South Wales Law Reform Commission (NSWLRC), *Privacy and Access to Personal Information: Points of Discussion* (2009)

New South Wales Law Reform Commission (NSWLRC), *Protecting Privacy in NSW* (2009)

New South Wales Law Reform Commission (NSWLRC), *Report 123 Privacy Principles* (2009)

New South Wales Law Reform Commission (NSWLRC), *Invasion of Privacy:* Report 120 (2009)

New South Wales Law Reform Commission (NSWLRC), *The Offices of the Information and Privacy Commissioner*: Report No 125 (2009)

New South Wales Law Reform Commission and Office of the Information and Privacy Commissioners, *Joint Report: Freedom of Information* (2009)

New South Wales Ombudsman's Office, *Review of Freedom of Information Act 1986: A Discussion Paper* (2008)

New South Wales Ombudsman's Office, *Review of Freedom of Information Act 1998* (2009)

Nurses Registration Board of New South Wales, *Professional Conduct* (NSW Nurses Registration Board, 2001)

Nursing and Midwifery Board of Australia, *Code of Professional Conduct for Nurses*, 5 (online) (current)

Office of the Australian Information Commission (OAIC), *Privacy Assessment Guide* (2006)

Office of the Australian Information Commissioner (OAIC), *Privacy Impact Assessment Guide* (Revised May 2010)

Office of the Australian Information Commissioner (OAIC), *Data Notification: A Guide to Handling Personal Information Security Breaches* (2011)

Office of the Australian Information Commission (OAIC), *The E-Health Record System* (2011)

Office of the Australian Information Commission, 'Australians Better Protected with Mandatory Data Breach Notification' (Media Release, 28 May 2013)

Office of the Australian Information Commission (OAIC), *Data Breach Notification: A Guide to Handling Personal Information Security Breaches* (2013)

Office of the Australian Information Commission (OAIC), *My Health Information – What are Health Service Providers?* (2013)

Office of the Australian Information Commission, *Australian Privacy Principles Guidelines: Privacy Act 1988 (Cth)* (1 March 2014)

Office of the Australian Information Commissioner (OAIC), *The E-Health Record System* (current)

Office of the Australian Privacy Commissioner (OAPC), to the Senate Legal and Constitutional Affairs Committee, on *Submission on the Healthcare Identifiers and Privacy: Discussion Paper on Proposal for Legislative Support* (12 August 2009)

Office of the NSW Privacy Commissioner, *Submission G118* (18 March 2002)

Office of the NSW Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005)

Office of the Victorian Privacy Commissioner, to the Senate Legal and Constitutional Affairs Committee, *Submission to Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, 20 June 2012

Office of the Victorian Privacy Commissioner, to Senate Standing Committee on Legal and Constitutional Affairs, Parliament of Australia on *Serious Invasions of Privacy in the Digital Era*, 9 July 2012

Parliament of the Commonwealth of Australia, *Explanatory Memorandum*, 'Personally Controlled Electronic Health Records Bill 2011'
Parliament of the Commonwealth of Australia, *Explanatory Memorandum*, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012'

Parliament of the Commonwealth of Australia, *Explanatory Memorandum*, 'Privacy Amendment (Privacy Alerts) Bill 2013'

Queensland Health, *Queensland Health Public Patients' Charter* (2002)

Roxon, Nicole, Minister for Health and Ageing, *Minister's Introduction' in National Health Reform 'Concept of Operations: Relating to the Introduction of Personally Controlled Electronic Health Record Systems* (2011) 3

Royal Australian College of General Practitioners, *Computer and Information Security Standards* (October 2011)

Royle, Richard, Steve Hambleton and Andrew Walduck, Panel Members, *Review of the Personally Controlled Electronic Record* ('Royle Review') (December 2013)

Senate Standing Committee on Constitutional and Legal Affairs, *A Bill of Rights for Australia?* (1985).

Senate Standing Committee on Constitutional and Legal Affairs, *Healthcare Identifiers Bill 2010 (Cth)*, 2010

Senate Standing Committee on Constitutional and Legal Affairs, *Provisions Healthcare Identifiers (Consequential Amendments) Bill 2011 (Cth),* March 2010

Senate Finance and Public Administration Legislation Committee (Cth), *Report Part 1: Australian Privacy Principles* (15 June 2011)

State Records New South Wales, *Issue Paper: Review of State Records Act 1998* (2004)

Strata Health Solutions, *Aligning Health Information System Design with Provincial and Federal EHR Initiatives*: *White Paper* (August 2003)

Victorian Government, Department of Health, *Public Hospital Patient Charter* (2009)

Victorian Privacy Commissioner, 'Federal Privacy Law Changes Welcome but Does Not Affect Victorian Privacy Legislation' (Media Release, 21 March 2014)

Victorian Law Reform Commission (VLRC), *Surveillance in Public Places*: Final Report No 18 (2010)

Victorian Law Reform Commission, *Privacy Law: Options for Reform Information Paper* (2001)

Queensland Clinical Trials Network, Independent Human Research Ethics Committee (HREC) (2012)

Western Australian Attorney-General, *Privacy Legislation for Western Australia* (2004)

Willison, Donald, 'Use of Data from the Electronic Health Record for Health Research – Current Governance Challenges and Potential Approaches' (March 2009) http://www.priv.gc.ca/information/pub/ehr-200903_e.pdf

E INTERNATIONAL MATERIALS

Asia-Pacific Economic Cooperation (APEC)

Asia Pacific Healthcare Informatics Agreement between China, New Zealand and Australia (signed in 1994)

Burns, Peter, *The Law and Privacy: The Canadian Experience* (2012) <http://www.privacylawyer.ca/2012/01/ontario> (viewed on 3/5/2012)

Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role: Final Report on the State of the Health Care System in Canada* (2010)

Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Federal Role in Health Infrastructure: Ottawa* ('The White Paper') (October 2002)

Canada, Department of Health, 'National Physician Survey' (2010) in The Commonwealth Fund, *International Profiles of Health Care Systems 2013* (December 2013)

Canada, Correctional Service Canada, 'Citizen Advisory Committees' http://www.csc-scc.gc.ca/cac/index-end.shtml (viewed on 12/8/2015)

Cavoukian, Ann, Angus Fisher, Scott Killen and David Hoffman, "Remote Home Health Care Technologies: How to Ensure Privacy? Build it in: privacy by Design" (22 May 2010) *Springerlink.com* (online)

Cavoukian, Ann, 'Embedding Privacy into Health Information Technology: An Absolute Must' (Paper Presented at MD Physician Services User Conference, 4 June 2010) http://www.ipc.on.ca/images/Resources/2010-06-04-Cdn_Medical_Association.pdf

Cavoukian, Ann, Information and Privacy Commissioner of Ontario, Canada, *Submission of the Information and Privacy Commissioner, Response to the FTC Framework for Protecting Consumer Privacy in an Era of Rapid Change* (21 January 2011)

Cavoukian, Ann and K El Eman, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* (June 2011)

Cavoukian, Ann, 'Privacy by Design: Strong Privacy Protection – Now and Well into the Future' (Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners Report, 2011)

Cavoukian, Ann, Information & Privacy Commissioner Canada and Richard C. Alvarez, President & CEO Canada Health Infoway, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities - Win/Win* (Discussion Paper, Information and Privacy Commissioner, Ontario, Canada, March 02 2012) http://www.ipc.on.ca/images/Resources/pbd-ehr-e_1.pdf

Cavoukian, Ann, *Reject Unlawful Surveillance – Stand Up for Privacy and Freedom of Design* (28 February 2014)

Cavoukian, Ann, Information and Privacy Commissioner of Ontario, Canada, *Privacy by Design in the Age of Big Data* (12 June 2014)

Canadian Government, Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada* (2012)

Canadian Government, Office of the Privacy Commission and Office and Provincial Office of Information, *Memorandum of Understanding* (2000) current as to 2015

Canada Health Info*way*, *EHRS Blueprint: An Enterprise Architecture for Sharing Electronic Health Records* (2011)<http://www.infoway-inforoute.ca> (viewed on 2/3/2012)

Council of Europe Charter on Education for Democratic Citizenship and Human Rights Education, Recommendation CM/Rec (2010) 7 and Explanatory Memorandum

United Nations Charter Article 1(3) (1945), Charter of the *United Nations*, opened for signature 26 June 1945, Australian Treaty Series 1945 No 1 (entered into force 24 October 1945, entered into force for Australia 1 November 1945)

Clarke, Roger, *Beyond the OECD Guidelines: Privacy Protection for the 21st Century* (4 January 2000) http://www.rogerclarke.com/DV/PP21C.html

Declaration of Geneva, Editorial Revision 2006, 173th Council Session of the World Medical Organisation, Divonne-les-Bains

Doupi, P, 'E-Health Strategies Country Brief: Denmark' (Report, European Commission, October 2010) http://ehealth-strategies.eu/database/denmark.html

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

Directive 2000/31/EC of the European Parliament and of the Council 2000 on the protection of individuals with regard to processing of personal data.

Directive 1997/66/EC of the European Parliament and the Council of 1997 on process of personal data and the protection of privacy in the telecommunication sector.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/0031

Education for Democratic Citizenship (EDC) at the Council of Europe – Information Sheet http://www.coe.int/t/dg4/education/edc/1_What_is_EDU_HRE/What_%20is_EDC_en.asp#TopOfPage

E-Health ERA, *E-Health Strategy and Implementation in Germany* (30 June 2007)

E-Health Europe, *Germany's National e-Health Programme: Contested but Driven Forward* (17 June 2012)

E-Health Care Solution, *Denmark Strategic Perspective* (2008) <http://www.e-healthsolution.com/denmark.aspx>

E-Health ERA, 'e-Health Strategy and Implementation Activities in Germany' 30 June 2007, <http://www.ehealth-era.org/database/documents/ERA_Reports/Germany-EH-ERA_Country_Report_fina>

E-Health Europe, 'Germany's National e-Health Programme: Contested but Driven Forward' 17 June 2012, <http://www.ehealtheurope.net/Features/item.cfm?docId=189>

E-Health Insider, *EMRs in Germany: Who will be in Charge?* (17 June 2012) <http://www.ehi.co.uk/features/item.cfm?docId=190>

E-Health Insider, *Germany: Health IT on the Rise* (17 June 2012) <http://www.ehealtheurope.net/features/germany/>

E-Health Insider, *Germany's National e-Health Programme: Contested but Driven Forward* (17 June 2012) http://www.ehi.co.uk/features/item.cfm?docId=189

E-Health Care Solution, *Denmark Strategic Perspective* (2008) <http://www.e-healthsolution.com/denmark.aspx>

E-Health ERA, *E-Health Strategy and Implementation Activities in Germany'* (30 June 2007) <http://www.ehealth-era.org/database/documents/ERA_Reports/Germany-EH-ERA_Country_Report_fina>

E-Health Europe, *Germany's National e-Health Programme: Contested but Driven Forward'* (17 June 2012) <http://www.ehealtheurope.net/Features/item.cfm?docId=189>

E-Health Insider, *EMRs in Germany: Who will be in Charge?* (17 June 2012) <http://www.ehi.co.uk/features/item.cfm?docId=190>

E-Health Insider, *Germany: Health IT on the Rise* (17 June 2012) <http://www.ehealtheurope.net/features/germany/>

E-Health Insider, *Germany's National e-Health Programme: Contested but Driven Forward* (17 June 2012) <http://www.ehi.co.uk/features/item.cfm?docId=189>

Emergency Management Information System and Reference Index

European Convention of Human Rights and Fundamental Freedom (1950) as amended by Protocol 11 (1998) and Protocol No 14 (2010) opened for signature 13 May 2004, Council of Europe Treaty Series No 194 (entered into force 1 June 2010), European Convention of Human Rights, *International Code of Medical Ethics Declaration of Geneva* (1950)

European Council, *Framework on Combating Terrorism*, 13 June 2003, [2000] OJL 164,

European Council, Preamble, *Guidelines on Human Rights and the Fight Against Terrorism*, adopted by the Committee of Ministers of the Council of Europe on 11 July 2002

European Union Commission, *Right to be Forgotten Ruling* (c-131/12)

Fichman, Robert, Rajiv Kohli and Ranjani Krishnan, "The Role of Information Systems in Healthcare: Current Research and Future Trends" (September 2011) 22(3) *Information System Research* 419.

Fraser, David, 'Ontario Recognizes Tort of Invasion of Privacy' in David Fraser, *Canadian Privacy Law Blog* (18 January 2012) http://blog.privacylawyer.ca/2012/01/ontario-recognizes-tort-of-invasion-of.html (viewed on 20/6/2012)

Hawkey, Kirstie and Kori Inkpen, 'Keeping Up Appearances: Understanding the Dimensions of Incidental Information Privacy' (Paper Presented at CHI Proceedings, Montreal Quebec, Canada, 22 April 2006, 821)

Health Canada, *Health Care Systems: eHealth* (9 August 2010) http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/index-eng.php

Hickford Mark, 'A Conceptual Approach to Privacy' (Miscellaneous Paper No 19, New Zealand Law Commission, October 2007) http://www.lawcom.govt.nz/sites/default/files/publications/2007/11/Publication_129_368_MP%2019.pdf (viewed on 11/5/2009)

Johansen, Ib and Med*Com*, *E-Health and implementation of EHR* (26 April 2006)

Klein, Sarah, Martha Hostetter and Douglas McCarthy, *A Vision for Using Digital Health Technologies to Empower Consumers and Transform the U.S. Health Care System* (October 2014)

Lium, Jan Tore and Arild Faxvaag, 'Removal of Paper-Based Health Records from Norwegian Hospitals: Effects on Clinical Workflow' (Report Norwegian Research Centre for Electronic

Patient Records, Faculty of Medicine, Norwegian University of Science and Technology, Trondheim, Norway, 2006)

Ludwick, D A and John Doucette, "Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Informations Systems Implementation Experiences in Seven Countries" (2009) 78 *International Journal of Medical Informatics* 22.

Med*Com*, *Denmark E-Health and Implementation of EHR* Hall in Tirol (26 April 2006) http://www.ehealth-benchmarking.org/2006/images/stories/06-johansen_denmark.pdf (viewed on 16/6/2012)

Metropolitan DC Police Department, 'Citizens Advisory Councils' (CAC) http://mpdc.dc.gov/page/citizens-advisory-councils-csc (viewed on 12/8/2015)

Ministerial Review Group Report (NZ), *Meeting the Challenge: Enhancing Sustainability and the Patient and Consumer Experience within the Current Legislative Framework for Health and Disability Services in New Zealand* (2009)

National Board of Health and Welfare (Denmark), *National IT Strategies – Denmark, England and Canada* (Report, May 2009) http://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/8374/2009-126-152_2009126152.pdf> (viewed on 2/12/2013)

National Board of Health Denmark, *National Strategy for Information Technology in the Health Care System 2003-2007* (Report, 2002) http://www.sst.dk/publ/Publ2004/National_IT_strategy.pdf (viewed on 2/12/2013)

National Board of Health, Denmark, *National Strategy for Information Technology in the Health Care System,* (2003-2007) (Report, 2002) <http://www.opencg.net/WS1_slides/S3_3_kvrneland/S3_arne.pdf> (viewed on 2/12/2013)

National Health Services (NHS), (UK), *Connecting for Health Spine* (2012) http://www.connectingforhealth.nhs.uk/systemsandservices/spine

New Zealand Healthcare, *NZ Creates National Health IT Plan* (24 August 2011) <http://www.futuregov.asia/articles/2011/aug/24/nz-creates-national-health-it-plan>

New Zealand Government, *Health Information Strategy New Zealand* (2009)

New Zealand Government, *National Health IT Plan* (2011)

New Zealand Law Commission, *A Conceptual Approach to Privacy* (MP 19, 2007)

New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies, Review of the Law of Privacy Stage 3*: Report No 113 (2010)

New Zealand Law Reform Commission, *Review of Privacy Stage 4*, Part 2 (NZLRC 123, 2011)

New Zealand Law Commission, *Review of the Privacy Act 1993*: Report 123, (June 2011) http://www.lawcom.govt.nz/sites/default/files/publications/2011/08/web_pdf1_review-of-the-privacy-act-1993-webpdf-72dpi-chapter-7-appendix_2.pdf> (viewed on 9/5/2012)

New Zealand, Ministerial Review Group Report, Minister of Health Tony Rydall, *Meeting the Challenge: Enhancing Sustainability and the Patient and Consumer Experience Within the current legislative Framework for Health and Disability Services in New Zealand* (16 August 2009)

Office of the Privacy Commissioner of Canada, Annual Report to Parliament 2013-14, *Transparency and Privacy in the Digital Age: Report on the Privacy Act* (October 2014)

Office of the Privacy Commissioner of Canada, Special Report to Parliament, *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (January 2014)

Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada* (March 2009) <http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>

Participedia, Couter, Jason, Citizen Advisory Board (4 June 2010) http://participedia.net/en/methods/citizen-advisory-board (viewed on 12/8/2015)

Standing Senate Committee on Social Affairs, Science and Technology, Parliament of Canada, *The Health of Canadians – The Federal Role Final Report. Volume Six: Recommendations for Reform* (October 2002)

Stroetmann, J Artmann, V Stroetmann with D Protti, J Dumortier, S Giest, U Walossek and D Whitehouse, *European Countries on Their Journey Towards National E-Health Infrastructures: Final European Progress Report ICT for Health Unit* (European Commission, January 2011)

The Commonwealth Fund, *International Profile of Health Care Systems, 2013* (December 2013)

The Commonwealth Fund, *International Profile of Health Care Systems, 2010-2012* (December 2012)

UK Parliament, Comptroller and Auditor-General (C&AGs) Report, *Department of Health: The National Programme for IT in the NHS, HC (2005-2006)* (March 2006)

UK Parliament, House of Commons Committee of Public Accounts, *Department of Health: The National Programme for IT in the NHS Twentieth Report of Session 2006-2007* (26 March 2007) ('First Report')

UK Parliament, House of Commons Committee of Public Accounts Report, *The National Programme for IT in the NHS: An Update on the Delivery of Detailed Care Records System – Forty-Fifth Report* (July 2011) ('Second Report')

United Nations Charter Article 1(3) (1945), *Charter of the United Nations*, opened for signature 26 June 1945, Australian Treaty Series 1945 No 1 (entered into force 24 October 1945, entered into force for Australia 1 November 1945)

United Nations, Human Rights Committee, *General Comment No 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant* UN DocCCPR/C/21/Rev.1/Add.13,18 (26 May 2004)

United Nations (UN), *Universal Declaration of Human Rights* (1948), GA Res 217A, 3rd sess, 183rd plen mtg, UN DocA/810 at 71 (1948)

United Nations, *United Nations Declaration on Human Rights: International Covenant on Civil and Political Rights* (1966), Art 17

United Nations, *Convention on the Elimination of all Forms of Racial Discrimination* (ratified 1972)

United Nations (UN), *International Covenant on Civil and Political Rights* ('ICCPR') (ratified in Australia 13 November 1980), Article 17

United Nations, *United Nations Convention on the Rights of the Child* (ratified 1993), Article 17

United Nations, *Universal Declaration of Bioethics and Human Rights* (2005), 33rd Session of the UNESCO General Conference, 19 October 2005

United Nations, *Universal Declaration on the Human Genome and Human Rights* (1997), adopted by the General Conference of the United Nations Educational, Scientific and Cultural Organization on 11 November 1997; endorsed by GA Res 53/152, UN Doc A/Res/53/152 (1998)

United Nations, *International Declaration on Human Genetic Data* (2003), OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) reprinted in (1981) 20 *International Legal Materials* 422

United Nations, Declaration of Helsinki – *Ethical Principles for Medical Research Involving Human Subjects* (amended 2008), 59th WMA General Assembly, Seoul, Korea (October 2008)

United Nation, *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), Art 17

United Nations, *International Labour Organisation Constitution* (1919), ILO Convention No 1

United Nations, High Commission for Human Rights, *Training Manual on Human Rights Monitoring* (2001)

U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 Washington, DC: U.S. Government Printing Office (September 1993). www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/ota_pc.html

Valdez, Adrienne, *NZ Creates National Health IT Plan: Future Governance* (24 August 2011) <http://www.futuregov.asia/articles/2011/aug/24/nz-creates-national-health-it-plan/>

Vancouver Island Health Authority (Canada), *Canada Health Infoway, Strata Health Solutions Inc. and Cerner* (2003)

World Health Organization (WHO), *International Health Regulations* 2005, Art 2

World Trade Organization (WTO), *Dispute Settlement Understanding* 2003, Art 8.2

World Trade Organization (WTO), *Agreement on the Trade-Related Aspects of Intellectual Property Rights* (TRIPS)

F Cases and Determinations

Australia/UK

A-G v Guardian Newspaper (No 2) [1990] 1 AC 109

Attorney-General for Victoria (ex rel Dale and Ors) v Commonwealth and Ors (1945) 71 CLR 237

American Civil Liberties Union v Reno 929 F Supp 824

Argyll v Argyll [1965] 1 All ER 611

Attorney-General (Vic): Ex rel Dale v Commonwealth (*Pharmaceutical Benefits Case*) [1945] HCA 30

Aubry v Duclos (1996) 141 DLR (4th) 683

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

Austin v Commonwealth of Australia 2003 ATC 4042

Bank of NSW v The Commonwealth (1948) 76 CLR 1

Batistatos v Roads and Traffic Authority (NSW) [2006] HCA 27

Ben Grubb and Telstra Corporation Limited [2015] AlCom 35 (1 May 2015)

Bennett & Dix v Higgins (2006) ATC 404

Bird v Jones (1845) 7 QB 742

Breen v Williams (1996) 186 CLR 71

British Medical Association v Commonwealth (1949) 79 CLR 201

Bunyan v Jordan (1937) 57 CLR 10

Campbell v MGN Ltd [2004] 2 AC 457

Carrier v Bonham [2001] QCA 234

Carter v Egg and Egg Pulp Marketing Board (Vic) (1942) 66 CLR 557

Chan v Sellwood; Chan v Calvert [2009] NSWSC 1335

Chow Hung Ching v The King (1948) 77 CLR 449

Clyde Engineering Co Ltd v Cowburn (1926) 37 CLR 466

Commonwealth v Tasmania (1983) 158 CLR 183

Coultas v Victorian Railways Commissioner (1886) 12 VLR 895

Doe v Yahoo! 7 Pty Ltd [2013] QDC 181

Douglas v Hello! Ltd [2001] 2 All ER 289

Douglas v Hello! Ltd [2007] 2 WLR 920

Dye v Commonwealth Securities Ltd [2010] FCA 720

Edge Pty Ltd v Apple Computer Inc. (1986) 161 CLR 171

Gee v Burger [2009] NSWSC 149

Ettinghausen v Australian Consolidated Press Ltd (unreported, NSWCA, 13 October 1993)

Federal Council of the British Medical Association in Australia and Ors v Commonwealth and Ors (1949) 79 CLR 201

'EZ' and 'EY' [2015] AlCmr 23 (27 March 2015)

Federal Council of the British Medical Association in Australia and Ors v Commonwealth and Ors (1949) 79 CLR 201

Fontin v Katapodis (1962) 108 CLR 177

Emcorp Pty Ltd v Australian Broadcasting Corporation [1988] 2 Qd R 169

General Practitioners Society of Australia v Commonwealth (1980) 145 CLR 532

Giller v Procopets [2004] VSC 113

Giller v Procopets [2008] VSCA 236

Gorton v Australian Broadcasting Commissioner (1973) 22 FLR 181

Grannall v Marrickville Margarine (1955) 93 CLR 55

Greig v Greig [1966] VR 376

Grosse v Purvis [2003] QDC 151

Halsey v Esso Petroleum Ltd [1961] 2 All ER; [1961] 1 WLR 683

Health Care Complaints Commission v Khan [2008] NSWNMT 15

Health Insurance Commission v Peverill (1994) 179 CLR 226

Henderson v Radio Corporation Pty Ltd (1960) 60 SR NSW 576

Home Office v Wainwright [2003] UKHL 53; [2003] 3 WLR 1137

HRH Prince of Wales v Association of Newspapers Ltd [2006] EWHC 522

Hung Ching v The King (1948) 77 CLR 449

Hunter v Canary Wharf Ltd [1997] AC 655

Jane Doe v Australian Broadcasting Corporation [2007] VCC 281

Jaensch v Coffey (1984) 155 CLR 549

Janvier v Sweeney [1919] 2 KB 316

John Fairfax Publications Pty Ltd v Hitchcock [2007] NSWCA 364

Johnston v Australian Broadcasting Commission (1993) FLR 307

Jane Doe v Australian Broadcasting Board [2007] VCC 281

Kadian v Richards (2004) 61 NSWLR 222

Kalaba v Commonwealth [2004] FCA 763

Kartinyeri v Commonwealth (1998) 195 CLR 337

Khorasandjian v Bush [1993] QB 727

Kioa v West (1992) 177 CLR 550

Kitson v Playfair, The Times (23-28 March 1896)

Koowarta v Bjelke-Peterson (1982) 153 CLR 168

Lincoln Hunt Australia Pty Ltd v Willesee (1986) 4 NSWLR 457

Lord Bernstein v Skynews & General Limited (1977)

Mabo v Queensland (No2) (1992) 175 CLR 1

Minister of State for Immigration and Ethnic Affairs v Teoh (1995) 183 CLR 273

Moorgate Tobacco Co Ltd v Philip Morris Ltd (1984) 156 CLR 415

Moore-Mcquillan v Work Cover Corporation [2007] SASC 55

Mount Isa Mines Ltd v Pusey (1970) 125 CLR 383

Nationwide News Pty Ltd v Naidu (2007) 71 NSWLR 417

New South Wales v Commonwealth (2006) 229 CLR 1

Newton-John v Scholl-Plough (Australia) (1985) 11 FCR 233

Northern Territory v Mengel (1995) 185 CLR 309

Prince Albert v Strange (1849) I H & Tw 1

Queensland and New South Wales Government v Commonwealth (2007)

R v Davidson [1969] VR 667

R v Kidman (1915) 20 CLR 425

R v Public Vehicle Licensing Appeal Tribunal (Tas); Ex parte Australian National Airways Pty Ltd (1964) 113 CLR 207

Raciti v Hughes (1995) 7 BPR 14

Richards v Kadian (2005) 64 NSWLR 204

Rogers v Nationwide News Pty Ltd (2003) 216 CLR 327

Rogers v Whitaker (1992) 175 CLR 479

Royal Melbourne Hospital v Mathews (1991) *Australian Health and Medical Reporter* 27-770.42

Women's Hospital v Medical Practitioners Board of Victoria [2005] VSC 225

Saad v Chubb Security Australia Pty Ltd [2012] NSWSC 1183

Sands v State of South Australia [2013] SASC 44

Sankey v Whitlam (1978) 142 CLR 1

Seager v Copydex [1967] 1 WLR 923 [658]

Secretary, Department of Health and Community Services (NT) v JWB (1992) 175 CLR 218

Slatter v Bissett (1986) 69 ACTR 25

Smith Kline & French Laboratories (Aust) v Secretary, Department of Community Services and *Health* (1990) 22 FCA 73.

South Australia v Commonwealth (1957) 99 CLR 373

Stephens v Avery [1988] 2 All ER 477 at 482

Tame v New South Wales (2002) 211 CLR 317

Triquet v Bath (1764) 3 Burr 1478

Union Steamship Co of Australia Pty Ltd v King (1988) 166 CLR 1

University of Wollongong v Metwally (1984) 158 CLR 447

Victoria v Commonwealth (1957) 99 CLR 575

Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479; [1937] ALR 597

Union Steamship Co of Australia Pty Ltd v King (1988) 166 CLR 1

University of Wollongong v Metwally (1984) 158 CLR 447

Victoria v Commonwealth (1957) 99 CLR 575

W v Egdell [1990] Ch. 359 at 389

Wainwright v Home Office [2004] 2 AC 406

Whisksoda Pty Ltd v HSV Channel 7 Pty Ltd (Victorian Supreme Court, McDonald J, 9417/93, 5 November 1993

Wilkinson v Downton [1897] 2 QB 57

Williams v Commonwealth of Australia [2014] HCA 23 (19 June 2014)

Williams v Commonwealth of Australia [2012] HCA 23 (20 June 2012)

Williams v Milotin (1957) 97 CLR 465

Wong v Parkside Health NHS Trust [2003] 3 All ER 932

New Zealand Cases:

Bradley v Wingnut Films [1993] 1 NZLR 415

C v Holland [2012] 3 NZLR 672

Duncan v Medical Practitioners Disciplinary Committee [1986] 1 NZLR 513

Furniss v Fitchet [1958] NZLR 396

Hosking v Runting [2004] NZCA 34

Hosking v Runting [2005] 1 NZLR 1; [2004] NZCA 34

P v D [2000] 2 NZLR 591

Tucker v News Media Ownership Ltd [1986] 2 NZLR 716 [731-733]

Canadian Cases:

Burnett v The Queen in right of Canada (1979) 94 DLR (3d) 281

Collins v Wilcock [1984] 1 WLR 1172

Cruise v Southdown Press (1993) 26 IRP 125

Jones v Tsige [2012] ONCA 32

Mallett v Shulman (1991) 2 Med LR 162

Maynes v Casey [2011] HCASL 173 (26 October 2011)

Motherwell v Motherwell (1976) 73 DLR (3d) 62

Ontario (Attorney-General) v Dieleman (1994) 117 DLR (4th) 449

U.S Cases:

Griswold v Connecticut (1965) 381 U.S. 479

Katz v United States 389 U.S. 347 (1967)

Kaye v Robertson [1991] FSR 62

Olmstead v United States 277 U.S. 438, 466 (1928)

People v Poddar, 10 Cal. 3d 750, 518 P

Roe v Wade (1973) 410 U.S. 113

*Smith v Jones (*1999) 132 CCC (3d) 225

Tarasoff v Regents of the University of Southern California (1976) 551 P 2d 334 (1976)

United States of America v Karl Brandt

UN Cases:

MS v Sweden (1997) 45 BMLR 133 (ECtHR)

Von Hannover v Germany [2004] ECHR 294

Z v Finland (1997) 25 EHRR 371 (ECtHR)

G Legislation

Australia:

Aboriginal and Torres Strait Islander Heritage Protection Act 1984 (Cth)

Archives Act 1983 (Cth)

Archives Amendment Act 2008 (Cth)

Australian Competition and Consumer Act 2010 (Cth)

Australian Constitution

Australia Act 1986 (Cth)

Australian Capital Territory (Self-Government) Act 1988 (Cth)

Australia Constitution Act 1900 (UK)

Australian Constitution Act 1901 (Imp)

Australian Postal Corporation Act 1989 (Cth)

Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 (Cth)

Cancer Act 1958 (Vic)

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Children and Young Persons (Care and Protection) Act 1998 (NSW)

Children (Care and Protection) Act 1987 (Cth)

Civil Dispute Resolution Act 2011 (Cth)

Civil Law (Wrongs) Act 2002 (ACT)

Civil Liability Act 2002 (NSW)

Civil Liability Act 1936 (SA)

Civil Liability Act 2002 (Tas)

Commonwealth of Australia Constitution Act 1900

Competition and Consumer Act 2010 (Cth)

Constitution Act 1902 (NSW)

Crimes Act 1900 (NSW)

Crimes Act 1914 (Cth)

Crimes Act 1958 (Vic)

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) *2004* (Cth)

Criminal Code 1899 (Qld)

Criminal Code 2002 (ACT)

Criminal Code 1924 (Tas)

Criminal Code Act 1913 (WA)

Criminal Code Act 1983 (NT)

Criminal Code Act 1913 (WA)

Criminal Code Act 1983 (NT)

Criminal Code Act 1995 (Cth)

Criminal Law Consolidation Act 1935 (SA)

Data-Matching Program (Assistance and Tax) Act 1990 (Cth)

Defamation Act 2005 (Cth)

Defamation Act 2005 (NSW)

Defamation Act 2006 (NT)

Defamation Act 2005 (Qld)

Defamation Act 2005 (SA)

Defamation Act 2005 (Tas)

Defamation Act 2005 (WA)

Defamation Act 2005 (Vic)

Evidence Act 1958 (Vic)

Evidence Act 1995 (NSW)

Evidence Act (Confidential Communication) Amendment Act 1999 (SA)

Fair Work Act 2009 (Cth)

Financial Management and Accountability Act 1997 (Cth)

Financial Transaction Reports Act 1988 (Cth)

Freedom of Information Act 1989 (Cth)

Freedom of Information Regulations 2000 (ACT)

Freedom of Information (Exempt Agency) Regulations 1993 (SA)

Freedom of Information Act 1987 (ACT)

Freedom of Information Act 1989 (NSW)

Freedom of Information Act 1992 (Qld)

Freedom of Information Act 1991 (SA)

Freedom of Information 1991 (Tas)

Freedom of Information Act 1982 (Vic)

Freedom of Information Act 1992 (WA)

Freedom of Information Amendment (Reform) Act 2010 (Cth)

Health Act 1958 (Vic)

Health Act 1993 (ACT)

Health Act 1911 (WA)

Health (Amendment) Act 1994 (ACT)

Health Administration Act 1982 (NSW)

Health Care Complaints Act 1993 (NSW)

Healthcare Identifiers Act 2010 (Cth)

Healthcare Identifiers Regulations 2010 (Cth)

Health Insurance Act 1973 (Cth)

Health Insurance Amendment Act 1977 (Cth)

Health (Regional Boards) Amendment (Medicare Agreement) Act 1993 (Tas)

Health Practitioner Regulation National Law Act 2009 (Cth)

Health Records Act 2001 (Vic)

Health Records Information Regulations 2012 (Vic)

Health Records and Information Privacy Act 2002 (NSW)

Health Records and Information Privacy Regulations 2010 (NSW)

Health Records (Privacy and Access) Act 1997 (ACT)

Health Services Act 1988 (Vic)

Healthcare Act 2008 (SA)

Healthcare Identifiers Act 2010 (Cth)

Healthcare Identifiers (Consequential Amendments) Act 2010 (Cth)

Health Ombudsman Act 2013 (Qld)

HIV/AIDS Preventative Measures Act 1993 (Tas)

Human Rights Act 2004 (ACT)

Human Rights (Parliamentary Scrutiny) Act 2012 (Cth)

Human Services Legislation Amendment Act 2011 (Cth)

Human Tissue and Transplantation Act 1982 (Cth)

Information Act 2002 (NT)

Information Privacy Act 2000 (Vic)

Information Privacy Act 2009 (Queensland)

Information Privacy Bill 2007 (WA)

Income Tax Act 1942 (Cth)

Income Tax (Wartime Arrangements) Act 1942 (Cth)

Income Tax Assessment Act 1942 (Cth)

Judicial Proceedings Report Act 1958 (Vic)

Medicare Principles and Commitments Act 1994 (Qld)

National Health Act 1953 (Cth)

National Health (Pharmaceutical Benefits) Regulations 1960 (Cth)

National Health (Pharmaceutical Benefits) Amendment Regulations (No 1) *2003* (Cth)

National Security Act 2007 (Cth)

Northern Territory (Self-Government) Act 1978 (Cth)

NSW State Records Act 1998

Notifiable Diseases Act 1981 (NT)

Ombudsman (Northern Territory) Act 1977 (NT)

Ombudsman Act 2001 (Qld)

Ombudsman Act 1972 (SA)

Ombudsman Act 1978 (Tas)

Ombudsman Act 1973 (Vic)

Ombudsman Act 1974 (NSW)

Personally Controlled Electronic Health Records Act 2012 (Cth) (PCEHR)

Personal Information Protection Act 2004 (Tas)

Personal Information and Protection Act 2004 (NSW)

Personally Controlled Electronic Health Records Act 2012 (Cth)

Personally Controlled Electronic Health Records (Consequential Amendments) Act 2012 (Cth)

Pharmaceutical Benefits Act 1944 (Cth)

Pharmaceutical Benefits Act 1947 (Cth)

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Private Sector) Act 2000 (Cth)

Privacy Amendment (Privacy Alerts) Act 2013 (Cth)

Privacy and Personal Information Protection Act 2002 (NSW)

Privacy and Personal Information Protection Regulation 2000 (NSW)

Protected Disclosures Act 1994 (NSW)

Public Health Act 1991 (NSW)

Public Health Act 1993 (ACT)

Public Health Act 1997 (Tas)

Public Health (General) Regulations 2002 (NSW)

Public Records Act 1973 (Vic)

Public and Environmental Health Act 1987 (SA)

Public Finance and Audit Act 1983 (NSW)

Public Service Amendment Act 2013 (Cth)

Spam Act 2003 (Cth)

States Grants (Income Tax Reimbursement) Act 1942 (Cth)

States (Tax Sharing and Health Grants) Act 1981 (Cth)

State Records Act 1998 (NSW)

State Records Act 2000 (WA)

Summary Offences Act 1953 (SA)

Summary Offences Act 1988 (NSW)

Surveillance Devices Act 2004 (Cth)

Taxation Administration Act 1953 (Cth)

Tax Law Amendment (Confidentiality of Taxpayer Information) Act 2010 (Cth)

Telecommunication Devices Act 1997 (Cth)

Telecommunications (Interception and Access) Act 1997 (Cth)

Telecommunications Interception Legislation Amendment Act 2002 (Cth)

Territories Law Reform Act 2010 (Cth)

Uniform Evidence Act 2008 (Cth)

Whistlelowers Protection Act 1994 (Qld)

Whistleblowers Protection Act 2001 (Vic)

Workplace Relations Amendment (Work Choices) Act 2005 (Cth)

International:

Act on Processing Personal Data 2000 (Denmark)

An Act Respecting the Protection of Personal Information in the Private Sector 2015 (Quebec)

California Constitution

California Civil Code § 1708.8

Canadian Constitution 1982

Canada Act 1982 (UK)

Canadian Charter of Human Rights and Freedoms 1982, Schedule B

Charter of the United Nations Act 1945

Civil Code of Quebec, SQ 1991, c 64

Constitution of New Zealand 1986

Cyber-Safety Act, SNS 2013, c2 (Canada)

Danmarks Riges Grundlov [Constitutional Act of Denmark]

Data Privacy Act 1998 (UK)

Employment Equity Act 1984 (Canada)

Federal Data Protection Act 2009 (Germany)

Grundgesetz für die Bundesrepublik Deutschland [Basic Law of the Federal Republic of Germany]

Human Rights Act 1985 (Canada)

Human Rights Act 1993 (NZ)

Human Rights Act 1998 (UK)

Kongeriget Norges Grundlov [The Constitution of the Kingdom of Norway]

Montana Constitution

New Zealand Bill of Rights Act 1990 (NZ)

New Zealand Constitution 1986 (NZ)

Personal Data Act 2000 (Norway)

Personal Health Information Privacy and Access Act 2009 (New Brunswick, Canada)

Personal Health Information Protection Act 2004 (Ontario, Canada)

Personal Information Protection Act 2003 (Alberta, Canada)

Personal Information Protection Act 2003 (British Columbia, Canada)

Personal Information Protection and Electronic Documents Act 2000 (Canada)

Privacy Act 1983 (Canada)

Privacy Act, RSNL 1990, c373 (British Columbia)

Privacy Act, RSM 1987, c P125 (Manitoba)

Privacy Act, RSNL 1990, c P-22 (Newfoundland and Labrador)

Privacy Act, RSS 1978, c P-24 (Saskatchewan)

Privacy Act 1993 (NZ)

Privacy Act, RSBC 1996, c373 (British Columbia, Canada)

Privacy Act, RSM 1987, c P125 (Manitoba, Canada)

Privacy Act, RSS 1978, c P-24 (Saskatchewan, Canada)

Privacy Act, RSNL 1990, c P-22 (Newfoundland and Labrador, Canada)

Privacy Amendment Act 1993 (NZ)

Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK)

Private Registers Act 1978 (Denmark)

Public Authorities Act 1978 (Denmark)

United States Constitution

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) 2001

H Other

'Is Technology Changing the Doctor/Patient Relationship? *CNN* (online) with *WebMD.com*. 30 June 1999

'Seven Million Britons Lie to Their GP' *Daily Mail* (United Kingdom), 1 February 2013, 14

'Your Obligations, for the Records' *Medical Observer* (Australia), 28 September 2007, 43

Abbott, Tony, 'Better Health For All Australians' (Media Release, Australia, ABB011/06, 10 February 2006)

Bajkowski, J, 'Future is Fixed, Thank God' *Australian Financial Review* (Australia), 11 November 2010, 66

Bracey, Andrew, 'PCEHR Consent Concerns Rejected' *Medical Observer* (Australia), 23 August 2013, 10

Bracey, Andrew, 'Rich Should Cough-Up: Dutton' *Medical Observer* (Australia), 28 February 2014, 1

Bracey, Andrew, 'Who's Responsible for e-health?' *Medical Observer* (Australia), 30 August 2013, 1-2

Bradley, Antonio, 'New Privacy Law Brings with it More Caution for GPs' *Australian Doctor* (Australia), 27 September 2013, 8

Bramwell, Neil, 'Privacy Minefield' *Medical Observer* (Australia), 11 April 2014, 14

Bramwell, Neil, 'Participating or Hindering?' *Medical Observer* (Australia), 28 June 2013, 20

Braue, David, 'E-Record Support Comes at a Price' *Medical Observer* (Australia), 18 March 2011, 1

Cesta, Danielle, 'Hacking into Health Files' *Medical Observer*, (Australia), I February 2013, 14-15

Cesta, Danielle, 'More E-Health Tech Drama' *Medical Observer* (Australia), 12 April 2013, 11

Chadwick, Vince, 'Privacy Fears on APPs that Track You' *Sydney Morning Herald* (Australia), 19 September 2012, 18

Clarke, Roger, *Beyond the OECD Guidelines: Privacy Protection for the 21st Century* (4 January 2000) <http://www.rogerclarke.com/DV/PP21C.html>

Colyer, Sarah, 'E-health indemnity stand-off' *Australian Doctor* (Australia), 15 June 2012, 1

Cooper, A, 'Battle Rages over AFL Drug Claims' *Canberra Times* (Australia), 30 August 2007, 12

Daily Telegraph, 'Threat to Privacy in E-Health Records' *Daily Telegraph* (Australia), 28 August 2012, 12

Dearne, Karen, 'Poor Uptake for Healthcare Identifiers' *The Australian* (Australia), 28 October 2011, 48

Dearne, Karen, 'E-Health Shock for Roxon' *The Australian* (Australia), 29 July 2009, 51

Dearne, Karen, 'E-Health Could be a Reality by 2012' *The Australian* (Australia), 28 July 2009, 45

Dunlevy, Sue, 'Patients Will Have to Pay for e-Health' *The Australian* (Australia), March 20 2012, 6

East, Michael, 'A Record Revolution' *Australian Doctor* (Australia), 24 June 2011, 45

FamousPictures, *Dog Poop Girl* (18 January 2012) <http://www.famouspictures.org/index.php?title=Dog_Poop_Girl>

The Sorcerer's Apprentice, Fantasia (Movie), 1940 US Production, Walt Disney Company

Fraser, David, 'Canadian Privacy Law: Ontario Recognizes Tort of Invasion of Privacy' (January 2012) Blog http://blog.privacylawyer.ca/2012/01/ontario-recognizes-tort-of-invasion-of.html (viewed on 20/6/2012)

Foo, Fran, 'Team McKinsey Bags Major E-Health Deal' *The Australian* (Australia), 7 July, 2011, 36

Goldhill, Olivia, 'Britons Embrace CCTV Cameras' *The Telegraph* (UK), 6 November 2014, 1

Greenleaf, Graham, 'Quacking like a Duck: The National ID Card Proposal (2006) Compared with the Australia Card (1986-87)' (12 June 2006), draft form available from the *Cyberspace Law & Policy Centre* website http://www.cyberlawcentre.org (viewed on 8/8/2007)

Grubb, Ben, 'Abbott Government Uncomfortable with Freedom of Information' *Sydney Morning Herald* (Australia), 14 May 2014, 28

Hambleton, Steve, 'To All E-Health Questions the Answer Seems to be No' *Australian Doctor* (Australia), 8 June 2012, 22

Herrick, Chloe, 'Federal Government Sheds Light on Next Round of E-Health Record Funding' *Computerworld* (Australia), 7 October 2011

Hughes, J, 'Upload of NSH Records Suspended', *BBC News* (UK), 16 April 2010 (online) http://news.bbc.co.uk/2/hi/health/8625007.stm (viewed on 10/5/2011)

Jabour, Bridie, 'Australian Authors Join Call for UN Bill of Digital Rights to Protect Privacy' *The Guardian* (UK), 10 December 2013, 1

Kaye, Bryon and Andrew Bracey, 'Shock Mass Departure of NEHTA Leads' *Medical Observer* (Australia), 23 August 2013, 1

Kerbaj, Richard 'Forget the Doctor: Now the Internet Makes House Calls' *Medical Observer* (Australia), 9-10 April 2010, 27

Kissane, Karen, 'Please Take a Number' *Sydney Morning Herald* (Australia), Monday 20 September 2010, 8

Knott, Matthew and David Wroe, 'Laws to Reduce Hacking Under Metadata Plan' *The Sydney Morning Herald* (Australia), 1-2 November 2014, 9

Kramer, Kathy, 'When Are Records Private?' *Medical Observer* (Australia), 4 May 2007

Krim, Jonathan, 'Subway Fracus Escalates into Test of Internet's Power to Shame' *Washington Post* (United States), 7 July 2005, 1

Lewis, Paul, 'You're Being Watched: There's One CCTV Camera for Every 32 People in UK' *The Guardian* (UK), 3 March 2011 (online)

Medical Observer, "When Are Records Private?" (Media Release, Australia, 4 May 2007) 42

Moore, David, 'Health*Connect* is Dead. So Now What?' *New Matilda* (Australia), 1 February 2006, 1

Morrel, S, 'Dob in Mr Cruel, Docs Told' *Herald Sun Melbourne* (Australia), 21 May 1992

Moses, Asher, 'Software Takes Brain Power Out of Hacking' *The Sydney Morning Herald* (Australia), 28 July 2011, 23

Newton, Kate, 'PCEHR Deadline Chaos' *Australian Doctor* (Australia), 25 January 2013, 1

Newton, Kate, 'GP Clinic Stands Firm Against Extortion Attempt from Hackers' *Australian Doctor* (Australia), 18 January 2013, 4

O'Brien, Mark, 'GPs Demand e-Health Clarity' *Medical Observer* (Australia), 13 April 2012, 1, 4

O'Brien, Mark, 'Physios Launch Bid for E-Health Records Funds' *Medical Observer* (Australia), 23 March 2012, 6

Phillips, Nicky, 'Computing Team Takes Quantum Leap', *Sydney Morning Herald* (Australia), 20 September 2012, 40

Richards, Deb, 'Medical Groups Snubbed by E-Health Initiative' *Medical Observer* (Australia), 25 November 2005, 9

Sheppard, Amanda, 'Social Networking' *Australian Doctor* (Australia), 30 August 2013, 43

Smith, Paul, 'Will Universal Healthcare Survive the MBS Ice Age?' *Australian Doctor* (Australia), 3 April 2015, 3

Smith, Paul, 'Dutton's Legacy: The Anti-Health Minister' *Australian Doctor* (Australia), 12 January 2015, 18

Smith, Paul, 'Battle Won, But War Not Over: Short Consult Breakdown Can't Mask Uncertain Future', *Australian Doctor* (Australia), 23 January 2015, 1

Smith, Paul, 'Is the Private Health Push in the Public Interest?' *Australian Doctor* (Australia), 2 April 2014, 18

Smith, Paul, 'Where is Debate on the Health of Our Nation?' *Australian Doctor* (Australia), 13 August 2013, 18

Smith, Paul, 'Big Stick Looms Over e-Health' *Australian Doctor* (Australia), 18 May 2012, 3

Smith, Paul, 'Who Are the Real Winners in the E-Health Pay Deal?' *Australian Doctor* (Australia), 24 August 2012, 18

Smith, Paul, 'Exodus of Doctor's Adds to E-Health Uncertainty' *Australian Doctor* (Australia), 28 August 2013, 18

Smith, Paul, 'Doctors Quit NEHTA' *Australian Doctor* (Australia), 23 August 2013, 1-2

Smith, Paul, 'GP E-Health Funding Win' *Australian Doctor* (Australia), 31 August 2012, 1

Smith, Paul, 'GPs to be E-Record Guardians' *Australian Doctor* (Australia), 18 March 2011, 1

Smith, Paul, 'Non-Medical E-Health Curators Risky' *Australian Doctor* (Australia), 17 June 2011, 3

Smith, Paul, 'Patients to Censor Own E-Health Records' *Australian Doctor* (Australia), 22 April 2011, 2

Smith, Paul, 'Give Me Socialised Medicine Any Day' *Australian Doctor* (Australia), 17 August 2009 (online)

Swan, Norman, 'Doctor/Patient Relationship' the Health Report, *Radio National* (Australia) Monday 7 August 2000 http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s161105.htm

Van Santen, Jaquie, 'Keystroke Consults' *Medical Observer* (Australia), 9 February 2007, 18-19

Waleed, Aly, 'Coalition Needs a Heart Transplant, Not a Facelift' *Sydney Morning Herald* (Australia), 6 February 2015, 20

Watkins, David, 'Sony Apologies for PlayStation Privacy Breach and Boosts Security' *Herald Sun* (UK), 2 May 2011 (online) http://www.heraldsun.com.au/news/world/sony-apologies-for-playstation-privacy-breach (viewed 0n 1/8/2011)

Williams, Suzanne, 'GP Uploads First-Ever E-Health Records', *Australian Doctor* (Australia), 14 September 2012, 5

Zetler, Julie and Karolyn White 'Healthcare Identifiers Act: Issues for Research Ethics' (Paper Presented at Law and Medicine Conference Rhodes, Greece, on 18 September 2011)